This user guide documents AOS Release 8.9R2.
The functionality described in this guide is subject to change without notice.

The Alcatel-Lucent name and logo are trademarks of Nokia used under license by ALE. To view other trademarks used by affiliated companies of ALE Holding, visit: www.al-enterprise.com/en/legal/trademarks-copyright. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Neither ALE Holding nor any of its affiliates assumes any responsibility for inaccuracies contained herein. © Copyright 2022 ALE International, ALE USA Inc. All rights reserved in all countries.
## Contents

**About This Guide** .................................................................................................................. xxix
Supported Platforms ................................................................................................................ xxix
Who Should Read this Manual? ................................................................................................ xxix
When Should I Read this Manual? ............................................................................................ xxix
What is in this Manual? ............................................................................................................ xxxi
What is Not in this Manual? ..................................................................................................... xxxi
How is the Information Organized? ........................................................................................ xxxi
Text Conventions .................................................................................................................... xxxii
Documentation Roadmap ........................................................................................................ xxxiii
Related Documentation .......................................................................................................... xxxv
Technical Support .................................................................................................................. xxxvi

### Chapter 1 Ethernet Port Commands

- interfaces .......................................................................................................................... 1-1
- interfaces speed .............................................................................................................. 1-4
- interfaces crossover ........................................................................................................ 1-6
- interfaces duplex ............................................................................................................ 1-8
- interfaces alias ............................................................................................................... 1-10
- clear interfaces ............................................................................................................. 1-12
- interfaces max-frame-size ......................................................................................... 1-14
- interfaces inter-frame-gap ......................................................................................... 1-16
- interfaces flood-limit .................................................................................................. 1-18
- interfaces flood-limit action ..................................................................................... 1-20
- interfaces ingress-bandwidth .................................................................................... 1-22
- interfaces pause .......................................................................................................... 1-24
- interfaces link-trap ...................................................................................................... 1-26
- interfaces ddm ............................................................................................................ 1-28
- interfaces ddm-trap ..................................................................................................... 1-30
- interfaces wait-to-restore .......................................................................................... 1-32
- interfaces wait-to-shutdown ...................................................................................... 1-33
- interfaces eee .............................................................................................................. 1-35
- interfaces primary-port split-mode ......................................................................... 1-37
- interfaces port break-out .......................................................................................... 1-39
- interfaces fec .............................................................................................................. 1-41
- interfaces hybrid-mode ............................................................................................. 1-43
- interfaces loopback .................................................................................................... 1-45
- interfaces portgroup .................................................................................................. 1-47
- clear violation .............................................................................................................. 1-49
- violation recovery-maximum ..................................................................................... 1-51
- violation recovery-time .............................................................................................. 1-53
Chapter 2  Power over Ethernet (PoE) Commands ................................................. 2-1
lanpower service ....................................................................................... 2-3
lanpower port admin-state ............................................................... 2-5
lanpower type ....................................................................................... 2-6
lanpower power ................................................................................... 2-6
## Contents

- **Chapter 3** UDLLD Commands  
  - udld .......................................................... 3-1  
  - udld port .................................................... 3-2  
  - udld mode .................................................. 3-4  
  - udld probe-timer ........................................... 3-6  
  - udld echo-wait-timer ...................................... 3-8  
  - clear udld statistics port ................................. 3-10  
  - show udld configuration .................................. 3-12  
  - show udld configuration port ............................ 3-15  
  - show udld statistics port ................................. 3-18  
  - show udld neighbor port ................................. 3-20  
  - show udld status port .................................... 3-22  

- **Chapter 4** Source Learning Commands  
  - mac-learning ................................................ 4-1  
  - mac-learning flush ........................................ 4-2  
  - mac-learning flush domain all ....................... 4-4  
  - mac-learning flush domain vlan .................... 4-6  
  - mac-learning flush domain spb ..................... 4-8  
  - mac-learning flush domain vxlan .................... 4-10  
  - mac-learning flush domain l2gre .................... 4-12  
  - mac-learning flush domain local .................... 4-14  
  - mac-learning flush domain l2gre .................... 4-16
### Contents

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>VLAN Management Commands</th>
<th>5-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-learning static mac-address</td>
<td>4-18</td>
<td></td>
</tr>
<tr>
<td>mac-learning domain vlan static mac-address</td>
<td>4-20</td>
<td></td>
</tr>
<tr>
<td>mac-learning domain spb static mac-address</td>
<td>4-22</td>
<td></td>
</tr>
<tr>
<td>mac-learning domain vxlan static mac-address</td>
<td>4-24</td>
<td></td>
</tr>
<tr>
<td>mac-learning domain local static mac-address</td>
<td>4-26</td>
<td></td>
</tr>
<tr>
<td>mac-learning multicast mac-address</td>
<td>4-28</td>
<td></td>
</tr>
<tr>
<td>mac-learning aging-time</td>
<td>4-31</td>
<td></td>
</tr>
<tr>
<td>mac-learning mode</td>
<td>4-33</td>
<td></td>
</tr>
<tr>
<td>show mac-learning</td>
<td>4-34</td>
<td></td>
</tr>
<tr>
<td>show mac-learning domain all</td>
<td>4-38</td>
<td></td>
</tr>
<tr>
<td>show mac-learning domain vlan</td>
<td>4-41</td>
<td></td>
</tr>
<tr>
<td>show mac-learning domain spb</td>
<td>4-45</td>
<td></td>
</tr>
<tr>
<td>show mac-learning domain vxlan</td>
<td>4-48</td>
<td></td>
</tr>
<tr>
<td>show mac-learning domain l2gre</td>
<td>4-51</td>
<td></td>
</tr>
<tr>
<td>show mac-learning domain local</td>
<td>4-54</td>
<td></td>
</tr>
<tr>
<td>show mac-learning aging-time</td>
<td>4-57</td>
<td></td>
</tr>
<tr>
<td>show mac-learning learning-state</td>
<td>4-58</td>
<td></td>
</tr>
<tr>
<td>show mac-learning mode</td>
<td>4-60</td>
<td></td>
</tr>
<tr>
<td>mac-ping</td>
<td>4-61</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>High Availability VLAN Commands</th>
<th>6-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>server-cluster</td>
<td>6-2</td>
<td></td>
</tr>
<tr>
<td>server-cluster vlan</td>
<td>6-4</td>
<td></td>
</tr>
<tr>
<td>server-cluster mac-address</td>
<td>6-6</td>
<td></td>
</tr>
<tr>
<td>server-cluster ip</td>
<td>6-8</td>
<td></td>
</tr>
<tr>
<td>server-cluster igmp mode</td>
<td>6-10</td>
<td></td>
</tr>
<tr>
<td>server-cluster ip-multicast</td>
<td>6-12</td>
<td></td>
</tr>
<tr>
<td>server-cluster port</td>
<td>6-14</td>
<td></td>
</tr>
<tr>
<td>server-cluster linkagg</td>
<td>6-16</td>
<td></td>
</tr>
<tr>
<td>show server-cluster</td>
<td>6-18</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>VLAN Stacking Commands</th>
<th>7-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethernet-service svlan</td>
<td>7-3</td>
<td></td>
</tr>
<tr>
<td>ethernet-service service-name</td>
<td>7-5</td>
<td></td>
</tr>
<tr>
<td>ethernet-service nni</td>
<td>7-7</td>
<td></td>
</tr>
<tr>
<td>ethernet-service svlan nni</td>
<td>7-10</td>
<td></td>
</tr>
<tr>
<td>ethernet-service sap</td>
<td>7-12</td>
<td></td>
</tr>
<tr>
<td>ethernet-service sap uni</td>
<td>7-14</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>ethernet-service sap cvlan</td>
<td>7-16</td>
<td></td>
</tr>
<tr>
<td>ethernet-service sap-profile</td>
<td>7-18</td>
<td></td>
</tr>
<tr>
<td>ethernet-service sap sap-profile</td>
<td>7-21</td>
<td></td>
</tr>
<tr>
<td>ethernet-service uni-profile</td>
<td>7-23</td>
<td></td>
</tr>
<tr>
<td>ethernet-service uni-profile inbound 802.1ab</td>
<td>7-27</td>
<td></td>
</tr>
<tr>
<td>ethernet-service uni uni-profile</td>
<td>7-30</td>
<td></td>
</tr>
<tr>
<td>ethernet-service custom-L2-protocol</td>
<td>7-32</td>
<td></td>
</tr>
<tr>
<td>ethernet-service uni-profile custom-L2-protocol</td>
<td>7-35</td>
<td></td>
</tr>
<tr>
<td>ethernet-service mac-tunneling</td>
<td>7-37</td>
<td></td>
</tr>
<tr>
<td>ethernet-service svlan mac-tunneling</td>
<td>7-39</td>
<td></td>
</tr>
<tr>
<td>ethernet-service transparent-bridging</td>
<td>7-41</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service vlan</td>
<td>7-43</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service</td>
<td>7-46</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service sap</td>
<td>7-49</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service port</td>
<td>7-51</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service nni</td>
<td>7-54</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service nni l2pt-statistics</td>
<td>7-56</td>
<td></td>
</tr>
<tr>
<td>clear ethernet-service nni l2pt-statistics</td>
<td>7-58</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service uni</td>
<td>7-60</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service uni l2pt-statistics</td>
<td>7-62</td>
<td></td>
</tr>
<tr>
<td>clear ethernet-service uni l2pt-statistics</td>
<td>7-64</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service uni-profile</td>
<td>7-66</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service custom-l2-protocol</td>
<td>7-69</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service uni-profile l2pt-statistics</td>
<td>7-71</td>
<td></td>
</tr>
<tr>
<td>clear ethernet-service uni-profile l2pt-statistics</td>
<td>7-74</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service mac-tunneling</td>
<td>7-75</td>
<td></td>
</tr>
<tr>
<td>show ethernet-service sap-profile</td>
<td>7-77</td>
<td></td>
</tr>
<tr>
<td>loopback-test</td>
<td>7-79</td>
<td></td>
</tr>
<tr>
<td>show loopback-test</td>
<td>7-83</td>
<td></td>
</tr>
<tr>
<td>clear loopback-test counters</td>
<td>7-85</td>
<td></td>
</tr>
</tbody>
</table>

Chapter 8  Distributed Spanning Tree Commands ................................................. 8-1

spantree mode ........................................................................................................ 8-3
spantree protocol .................................................................................................... 8-5
spantree vlan admin-state .................................................................................... 8-7
spantree mst region name ..................................................................................... 8-9
spantree mst region revision-level ...................................................................... 8-11
spantree mst region max-hops .............................................................................. 8-13
spantree msti ......................................................................................................... 8-15
spantree msti vlan ................................................................................................ 8-17
spantree priority .................................................................................................... 8-19
spantree hello-time ............................................................................................... 8-22
spantree max-age .................................................................................................. 8-24
spantree forward-delay ......................................................................................... 8-26
spantree bpdu-switching ....................................................................................... 8-28
spantree path-cost-mode ....................................................................................... 8-30
spantree pyst+compatibility .................................................................................. 8-32
spantree auto-vlan-containment ........................................................................... 8-34
spantree cist ........................................................................................................... 8-36
spantree cist ............................................................................................................ 8-38
spantree cist path-cost ......................................................................................... 8-40
spantree msti path-cost ........................................................................................ 8-42
Chapter 9  Shortest Path Bridging Commands

spb bvlan ................................................................. 9-1
spb isis bvlan cct-id ................................................... 9-3
spb isis control-bvlan ............................................... 9-5
spb isis bvlan tandem-multicast-mode ...................... 9-7
spb isis bridge-priority ............................................ 9-9
spb isis interface ..................................................... 9-11
spb ipv6 bind ............................................................. 9-13
spb ipv6 redist .......................................................... 9-17
show spb ipv6 bind ................................................... 9-19
show spb ipv6 redist .................................................. 9-21
show spb ipv6 route-table ......................................... 9-23
show spb ipv66 bind .................................................. 9-25
show spb ipv66 redist ................................................ 9-27
show spb ipv66 route-table ....................................... 9-29
spb isis admin-state ............................................... 9-31
spb isis area-address .............................................. 9-33
spb isis source-id ...................................................... 9-35
spb isis control-address .......................................... 9-37
spb isis spf-wait ....................................................... 9-39
Chapter 10  Service Manager Commands

service spb .................................................................................................................. 10-1
service pseudo-wire .................................................................................................... 10-4
service vxlan .............................................................................................................. 10-7
service l2gre ............................................................................................................. 10-10
service description .................................................................................................. 10-13
service multicast-mode ........................................................................................... 10-16
service stats ............................................................................................................. 10-18
service vlan-xlation ............................................................................................... 10-21
service admin-state ................................................................................................. 10-23
service remove-ingress-tag .................................................................................... 10-25
service vxlan udp-port ............................................................................................ 10-27
service vxlan vrf ..................................................................................................... 10-29
service local-rrp ...................................................................................................... 10-31
service l2gre reserved-vlan .................................................................................... 10-33
service 3vpn profile ................................................................................................. 10-35
service l2profile .................................................................................................... 10-37
service l2profile inbound 802.1ab ........................................................................... 10-39
service access ........................................................................................................ 10-42
service access l2profile .......................................................................................... 10-44
service access vlan-xlation .................................................................................... 10-46
service sap ................................................................................................................ 10-49
service sap description ........................................................................................... 10-51
service sap trusted .................................................................................................. 10-53
service sap stats ...................................................................................................... 10-55
service sap admin-state ......................................................................................... 10-57
service sdp vxlan .................................................................................................... 10-59
service sdp l2gre .................................................................................................... 10-61
service bind-sdp ..................................................................................................... 10-63
service l2gre auto-discover .................................................................................... 10-65

show service spb ....................................................................................................... 9-56
show service pseudo-wire ....................................................................................... 9-59
show service vxlan .................................................................................................. 9-61
show service l2gre .................................................................................................. 9-64
show service description ....................................................................................... 9-67
show service stats ................................................................................................ 9-70
show service vlan-xlation ....................................................................................... 9-73
show service admin-state ....................................................................................... 9-76
show service remove-ingress-tag ......................................................................... 9-78
show service vxlan udp-port .................................................................................. 9-80
show service vxlan vrf ............................................................................................ 9-82
show service local-rrp ............................................................................................ 9-84
show service l2gre reserved-vlan ......................................................................... 9-86
show service 3vpn profile ....................................................................................... 9-88
show service l2profile inbound 802.1ab ................................................................ 9-90
Chapter 11  Loopback Detection Commands ........................................... 11-1
  loopback-detection ......................................................... 11-2
  loopback-detection port .................................................. 11-4
  loopback-detection service-access ................................. 11-6
  loopback-detection transmission-timer ......................... 11-8
  loopback-detection autorecovery-timer .......................... 11-10
  show loopback-detection ............................................... 11-12
  show loopback-detection port ....................................... 11-14
  show loopback-detection linkagg ................................... 11-17
  show loopback-detection statistics port ....................... 11-19
  clear loopback-detection statistics port ..................... 11-21

Chapter 12  Link Aggregation Commands ............................................. 12-1
  linkagg static agg size .................................................. 12-3
  linkagg static agg name ............................................... 12-6
  linkagg static agg wait-to-restore-time ...................... 12-8
  linkagg static agg loopback .......................................... 12-10
  linkagg static agg loopback internal ............................ 12-12
  linkagg static agg admin-state ..................................... 12-14
  linkagg static port agg .............................................. 12-16
  linkagg lacp agg size ................................................. 12-18
  linkagg lacp agg name ............................................... 12-21
  linkagg lacp agg wait-to-restore-time ....................... 12-23
  linkagg lacp agg admin-state ..................................... 12-25
  linkagg lacp agg actor admin-key ................................. 12-27
  linkagg lacp agg actor system-priority ....................... 12-29
  linkagg lacp agg actor system-id ............................... 12-31
  linkagg lacp agg partner system-id ............................. 12-33
**Chapter 13**

**Virtual Chassis Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-chassis configured-chassis-id</td>
<td>13-3</td>
</tr>
<tr>
<td>virtual-chassis chassis-group</td>
<td>13-5</td>
</tr>
<tr>
<td>virtual-chassis configured-chassis-priority</td>
<td>13-7</td>
</tr>
<tr>
<td>virtual-chassis configured-control-vlan</td>
<td>13-9</td>
</tr>
<tr>
<td>virtual-chassis configured-hello-interval</td>
<td>13-11</td>
</tr>
<tr>
<td>virtual-chassis vf-link create</td>
<td>13-13</td>
</tr>
<tr>
<td>virtual-chassis vf-link member-port</td>
<td>13-15</td>
</tr>
<tr>
<td>virtual-chassis vf-link default-vlan</td>
<td>13-17</td>
</tr>
<tr>
<td>virtual-chassis hello-interval</td>
<td>13-19</td>
</tr>
<tr>
<td>virtual-chassis shutdown</td>
<td>13-21</td>
</tr>
<tr>
<td>virtual-chassis vf-link-mode</td>
<td>13-23</td>
</tr>
<tr>
<td>virtual-chassis auto-vf-link-port</td>
<td>13-25</td>
</tr>
<tr>
<td>vc-takeover</td>
<td>13-27</td>
</tr>
<tr>
<td>ssh-chassis</td>
<td>13-29</td>
</tr>
<tr>
<td>convert configuration</td>
<td>13-30</td>
</tr>
<tr>
<td>show virtual-chassis topology</td>
<td>13-32</td>
</tr>
<tr>
<td>show virtual-chassis consistency</td>
<td>13-37</td>
</tr>
<tr>
<td>show virtual-chassis vf-link</td>
<td>13-40</td>
</tr>
<tr>
<td>show virtual-chassis auto-vf-link-port</td>
<td>13-42</td>
</tr>
<tr>
<td>show virtual-chassis chassis-reset-list</td>
<td>13-44</td>
</tr>
<tr>
<td>show virtual-chassis slot-reset-list</td>
<td>13-46</td>
</tr>
<tr>
<td>show virtual-chassis neighbors</td>
<td>13-48</td>
</tr>
<tr>
<td>show configuration vcm-snapshot chassis-id</td>
<td>13-50</td>
</tr>
</tbody>
</table>
Chapter 14  Ethernet Ring Protection Commands ........................................................... 14-1
  erp-ring .............................................................................................................. 14-2
  erp-ring rpl-node .............................................................................................. 14-6
  erp-ring wait-to-restore .................................................................................... 14-8
  erp-ring enable ................................................................................................. 14-10
  erp-ring guard-timer ......................................................................................... 14-12
  erp-ring sub-ring .............................................................................................. 14-14
  erp-ring virtual-channel .................................................................................... 14-17
  erp-ring revertive .............................................................................................. 14-19
  erp-ring clear .................................................................................................... 14-21
  erp-ring ethoam-event ...................................................................................... 14-23
  erp-ring sap-neighbor ....................................................................................... 14-25
  clear erp statistics ............................................................................................ 14-27
  show erp ........................................................................................................... 14-29
  show erp statistics ............................................................................................ 14-33

Chapter 15  Media Redundancy Protocol Commands .................................................. 15-1
  mrp ...................................................................................................................... 15-2
  mrp domain ...................................................................................................... 15-4
  mrtype............................. ............................................................................. 15-8
  show mrp ........................................................................................................... 15-12
  show mrp domain ............................................................................................ 15-16
  show mrp port .................................................................................................. 15-23
  show mrp interconnect ..................................................................................... 15-25
  clear mrp ......................................................................................................... 15-29
  clear mrp interconnect ..................................................................................... 15-31
  clear mrp port .................................................................................................. 15-33

Chapter 16  MVRP Commands .................................................................................... 16-1
  mvrp ................................................................................................................... 16-2
  mvrp port .......................................................................................................... 16-3
  mvrp linkagg ..................................................................................................... 16-5
  mvrp maximum-vlan ......................................................................................... 16-7
  mvrp registration .............................................................................................. 16-8
  mvrp applicant ................................................................................................. 16-10
  mvrp timer join ................................................................................................. 16-12
  mvrp timer leave .............................................................................................. 16-14
  mvrp timer leaveall .......................................................................................... 16-16
  mvrp timer periodic-timer ............................................................................... 16-18
  mvrp periodic-transmission ............................................................................. 16-20
  mvrp restrict-vlan-registration ....................................................................... 16-22
  mvrp restrict-vlan-advertisement ..................................................................... 16-24
  mvrp static-vlan-restrict .................................................................................. 16-26
Chapter 17 802.1AB Commands

- show mvrp configuration .......................................................... 16-28
- show mvrp port ......................................................................... 16-30
- show mvrp linkagg ................................................................. 16-33
- show mvrp timer ....................................................................... 16-35
- show mvrp statistics ................................................................. 16-38
- show mvrp last-pdu-origin ....................................................... 16-42
- show mvrp vlan-restrictions ..................................................... 16-44
- mvrp clear-statistics ................................................................. 16-46

- show lldp local-port power-via-mdi ......................................... 17-78
- show lldp local-port power-via-mdi-measurements ................. 17-83
- show lldp remote-system power-via-mdi .................................. 17-71
- show lldp remote-system power-via-mdi-measurements .......... 17-75
- show lldp remote-system power-via-mdi-local-port ................. 17-78
- show lldp remote-system power-via-mdi-local-port-measurements 17-83
- show lldp remote-system power-via-mdi-agent-destination-address 17-86
- lldp trust-agent ....................................................................... 17-88
- lldp trust-agent violation-action ............................................. 17-90
- show lldp trusted remote-agent .............................................. 17-92
- show lldp trust-agent ............................................................. 17-94

Chapter 18 SIP Commands

- sip-snooping admin-state .......................................................... 18-2
## Chapter 19  Automatic Fabric Commands

- auto-fabric admin-state ................................................................. 19-2
- auto-fabric interface ..................................................................... 19-4
- auto-fabric discovery start ........................................................... 19-6
- auto-fabric protocols ................................................................... 19-7
- auto-fabric config-save interval .................................................... 19-10
- auto-fabric config-save admin-state .............................................. 19-12
- auto-fabric discovery-interval ....................................................... 19-13
- auto-fabric protocols spb default-profile ...................................... 19-14
- auto-fabric protocols spb set-profile ........................................... 19-16
- show auto-fabric config ............................................................... 19-18
- show auto-fabric config interface ................................................ 19-21

## Chapter 20  IP Commands

- ip interface .................................................................................. 20-1
- ip interface rtr-port ..................................................................... 20-5
- ip interface tunnel ....................................................................... 20-9
- ip interface dhcp-client .............................................................. 20-11
- ip router primary-address ............................................................ 20-13
- ip router router-id ....................................................................... 20-16
- ip static-route ............................................................................. 20-17
- ip static-route all bfd-state ......................................................... 20-19
- ip static-route bfd-state .............................................................. 20-22
- ip route-pref ............................................................................... 20-23
- ip default-ttl .............................................................................. 20-25
- ping ............................................................................................ 20-27
- traceroute ................................................................................... 20-28
- ip directed-broadcast ................................................................. 20-30
- ip directed-broadcast trusted-source-ip ...................................... 20-32
- ip directed-broadcast clear ........................................................ 20-34
- show ip directed-broadcast ....................................................... 20-35
- ip service .................................................................................... 20-41
- ip service port ............................................................................ 20-43
- ip service source-ip .................................................................... 20-45
- ip redist ..................................................................................... 20-47
## Contents

- `ip access-list` .......................................................... 20-50
- `ip access-list address` ........................................ 20-52
- `ip route-map action` .................................................... 20-54
- `ip route-map match ip address` .......................... 20-56
- `ip route-map match ipv6 address` ...................... 20-58
- `ip route-map match ip-nexthop` ......................... 20-60
- `ip route-map match ipv6-nexthop` .................... 20-62
- `ip route-map match tag` ........................................... 20-64
- `ip route-map match ipv4-interface` ................... 20-66
- `ip route-map match ipv6-interface` .................... 20-68
- `ip route-map match metric` ..................................... 20-70
- `ip route-map match route-type` ...................... 20-72
- `ip route-map match protocol` ........................... 20-74
- `ip route-map match name` ..................................... 20-76
- `ip route-map set metric` ........................................ 20-78
- `ip route-map set metric-type` .................... 20-80
- `ip route-map set tag` ............................................. 20-82
- `ip route-map set community` ........................ 20-84
- `ip route-map set local-preference` .................. 20-86
- `ip route-map set level` ........................................ 20-88
- `ip route-map set ip-nexthop` ......................... 20-90
- `ip route-map set ipv6-nexthop` ...................... 20-92
- `ip route-map set ipv6-nexthop` ...................... 20-94
- `vrf` ........................................................................... 20-97
- `ip export` ................................................................. 20-99
- `ip import` ............................................................... 20-100
- `show ip export` .................................................. 20-103
- `show ip import` .................................................. 20-105
- `show ip global-route-table` ................................ 20-107
- `arp` ................................................................. 20-109
- `ip distributed-arp admin-state` ................ 20-111
- `arp send-gratuitous-arp` ..................................... 20-112
- `clear arp-cache` .................................................. 20-114
- `ip dos arp-poison restricted-address` .... 20-115
- `arp filter` ............................................................. 20-116
- `clear arp filter` ...................................................... 20-118
- `icmp type` ......................................................... 20-119
- `icmp unreachable` ................................................ 20-121
- `icmp echo` ........................................................... 20-123
- `icmp timestamp` .............................................. 20-125
- `icmp addr-mask` .................................................. 20-127
- `icmp messages` .................................................. 20-129
- `ip dos scan close-port-penalty` ................ 20-131
- `ip dos scan tcp open-port-penalty` .............. 20-133
- `ip dos scan udp open-port-penalty` ............ 20-135
- `ip dos scan threshold` ........................................ 20-137
- `ip dos trap` ........................................................ 20-139
- `ip dos scan decay` ............................................ 20-141
- `ip dos type` .......................................................... 20-143
- `ip tcp half-open-timeout` .................................. 20-145
- `ip tcp time-stamp-response` ....................... 20-146
- `show ip tcp time-stamp-response` ............. 20-147
- `show ip traffic` .................................................... 20-148
Contents

show ip interface ................................................................. 20-151
show ip emp-interfaces ....................................................... 20-158
show ip routes ................................................................. 20-160
show ip route-pref ............................................................ 20-163
show ip redist ................................................................. 20-165
show ip redist-routes ........................................................ 20-167
show ip access-list .......................................................... 20-169
show ip route-map ............................................................ 20-171
show ip router database ...................................................... 20-173
show ip emp-routes .......................................................... 20-176
show ip config ................................................................. 20-178
show ip protocols ............................................................. 20-180
show ip router-id .............................................................. 20-182
show ip service ................................................................. 20-184
show ip service source-ip .................................................... 20-186
show ip dos arp-poison ....................................................... 20-188
show arp ........................................................................... 20-190
show ip arp utilization ......................................................... 20-192
show arp filter ................................................................. 20-194
show arp send-gratuitous-arp ............................................. 20-196
show icmp control ............................................................. 20-198
show icmp statistics .......................................................... 20-200
show tcp statistics ............................................................ 20-202
show tcp ports ................................................................. 20-204
show ip tcp half-open-timeout ............................................. 20-206
show udp statistics ............................................................ 20-207
show udp ports ................................................................. 20-209
show ip dos config ............................................................ 20-211
show ip dos statistics ........................................................ 20-214
show vrf .......................................................................... 20-216
show vrf-profiles ............................................................. 20-219

Chapter 21 IPv6 Commands ......................................................... 21-1
ipv6 interface ................................................................. 21-3
ipv6 interface rtr-port ....................................................... 21-9
ipv6 interface tunnel source destination ................................. 21-11
ipv6 address ................................................................. 21-13
ipv6 address global-id ...................................................... 21-15
ipv6 address local-unicast ................................................ 21-17
ipv6 dad-check ............................................................... 21-19
ipv6 hop-limit ............................................................... 21-20
ipv6 pmhu-lifetime ......................................................... 21-22
ipv6 neighbor stale-lifetime .............................................. 21-23
ipv6 neighbor ............................................................... 21-24
ipv6 neighbor limit .......................................................... 21-26
ipv6 neighbor vrf-limit ..................................................... 21-28
ipv6 ra-filter ................................................................. 21-30
ipv6 ra-filter trusted ....................................................... 21-32
ipv6 prefix ................................................................. 21-34
ipv6 static-route ............................................................ 21-36
ipv6 static-route all bfd-state .......................................... 21-39
ipv6 static-route bfd-state ............................................... 21-40
## Contents

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 global-route-table</td>
<td>21-123</td>
</tr>
<tr>
<td>show ipv6 import</td>
<td>21-121</td>
</tr>
<tr>
<td>show ipv6 export</td>
<td>21-119</td>
</tr>
<tr>
<td>ipv6 import</td>
<td>21-116</td>
</tr>
<tr>
<td>show ipv6 redist-routes</td>
<td>21-109</td>
</tr>
<tr>
<td>show ipv6 redist</td>
<td>21-107</td>
</tr>
<tr>
<td>ipv6 access-list</td>
<td>21-105</td>
</tr>
<tr>
<td>ipv6 access-list address</td>
<td>21-103</td>
</tr>
<tr>
<td>show ipv6 redist address</td>
<td>21-101</td>
</tr>
<tr>
<td>show ipv6 redist-routes</td>
<td>21-109</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>21-111</td>
</tr>
<tr>
<td>ipv6 import</td>
<td>21-113</td>
</tr>
<tr>
<td>ipv6 export</td>
<td>21-116</td>
</tr>
<tr>
<td>show ipv6 export</td>
<td>21-119</td>
</tr>
<tr>
<td>show ipv6 import</td>
<td>21-121</td>
</tr>
<tr>
<td>show ipv6 global-route-table</td>
<td>21-123</td>
</tr>
<tr>
<td>ipv6 route-pref</td>
<td>21-42</td>
</tr>
<tr>
<td>ipv6 virtual-source-mac</td>
<td>21-44</td>
</tr>
<tr>
<td>ipv6 echo</td>
<td>21-46</td>
</tr>
<tr>
<td>ipv6 icmp rate-limit</td>
<td>21-47</td>
</tr>
<tr>
<td>ping6</td>
<td>21-49</td>
</tr>
<tr>
<td>traceroute6</td>
<td>21-51</td>
</tr>
<tr>
<td>modify boot parameters</td>
<td>21-53</td>
</tr>
<tr>
<td>show ipv6 icmp statistics</td>
<td>21-56</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>21-59</td>
</tr>
<tr>
<td>show ipv6 emp-interface</td>
<td>21-66</td>
</tr>
<tr>
<td>show ipv6 emp-routes</td>
<td>21-68</td>
</tr>
<tr>
<td>show ipv6 pmTu table</td>
<td>21-70</td>
</tr>
<tr>
<td>show ipv6 ra-filter</td>
<td>21-72</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>21-74</td>
</tr>
<tr>
<td>clear ipv6 neighbors</td>
<td>21-76</td>
</tr>
<tr>
<td>show ipv6 prefixes</td>
<td>21-77</td>
</tr>
<tr>
<td>show ipv6 routes</td>
<td>21-79</td>
</tr>
<tr>
<td>show ipv6 route-pref</td>
<td>21-81</td>
</tr>
<tr>
<td>show ipv6 router database</td>
<td>21-83</td>
</tr>
<tr>
<td>show ipv6 tcp connections</td>
<td>21-85</td>
</tr>
<tr>
<td>show ipv6 tcp listeners</td>
<td>21-87</td>
</tr>
<tr>
<td>show ipv6 traffic</td>
<td>21-89</td>
</tr>
<tr>
<td>show ipv6 tunnel configured</td>
<td>21-92</td>
</tr>
<tr>
<td>show ipv6 tunnel 6to4</td>
<td>21-94</td>
</tr>
<tr>
<td>show ipv6 udp ports</td>
<td>21-96</td>
</tr>
<tr>
<td>show ipv6 information</td>
<td>21-98</td>
</tr>
<tr>
<td>ipv6 redist</td>
<td>21-101</td>
</tr>
<tr>
<td>ipv6 access-list</td>
<td>21-103</td>
</tr>
<tr>
<td>ipv6 access-list address</td>
<td>21-105</td>
</tr>
<tr>
<td>show ipv6 redist</td>
<td>21-107</td>
</tr>
<tr>
<td>show ipv6 redist-routes</td>
<td>21-109</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>21-111</td>
</tr>
<tr>
<td>ipv6 export</td>
<td>21-113</td>
</tr>
<tr>
<td>ipv6 import</td>
<td>21-116</td>
</tr>
<tr>
<td>show ipv6 export</td>
<td>21-119</td>
</tr>
<tr>
<td>show ipv6 import</td>
<td>21-121</td>
</tr>
<tr>
<td>show ipv6 global-route-table</td>
<td>21-123</td>
</tr>
<tr>
<td>ip load rip</td>
<td>23-3</td>
</tr>
</tbody>
</table>

**Chapter 22**  
**IPsec Commands**  
- ipsec key  
- ipsec security-key  
- ipsec policy  
- ipsec policy rule  
- ipsec sa  
- ipsec default-discard  
- show ipsec policy  
- show ipsec sa  
- show ipsec key  
- show ipsec statistics

**Chapter 23**  
**RIP Commands**  
- ip load rip
Chapter 24  BFD Commands

ip bfd admin-state ................................................................. 24-2
ip bfd transmit ................................................................. 24-3
ip bfd receive ................................................................. 24-5
ip bfd multiplier ............................................................. 24-7
ip bfd echo-interval ......................................................... 24-9
ip|ipv6 bfd interface ......................................................... 24-11
ip|ipv6 bfd interface admin-state .................................. 24-13
ip|ipv6 bfd interface transmit ......................................... 24-15
ip|ipv6 bfd interface receive ........................................... 24-17
ip|ipv6 bfd interface multiplier ...................................... 24-19
ip|ipv6 bfd interface echo-interval .................................. 24-21
Chapter 25  DHCP Relay Commands

show ip bfd ................................................................. 24-23
show ipv6 bfd interfaces ........................................ 24-25
show ipv6 bfd sessions ............................................ 24-27
show ipv6 bfd sessions statistics ......................... 24-30

ip dhcp relay admin-state ......................................... 25-4
ip dhcp relay destination ......................................... 25-6
ip dhcp relay per-interface-mode ............................ 25-8
ip dhcp relay interface destination ....................... 25-10
ip dhcp relay interface admin-state ...................... 25-12
ip dhcp relay forward-delay .................................... 25-14
ip dhcp relay maximum-hops ................................. 25-16
ip dhcp relay insert-agent-information .................. 25-18
ip dhcp relay insert-agent-information policy ........ 25-20
ip dhcp relay insert-agent-information format ....... 25-22
ip dhcp relay pxe-support ...................................... 25-25
show ip dhcp relay interface ................................. 25-26
show ip dhcp relay statistics ................................. 25-29
ip dhcp relay clear statistics ................................. 25-31
show ip dhcp relay insert-agent-information error-count 25-33
ip dhcp relay clear insert-agent-information error-count 25-35
show ip dhcp relay counters ................................. 25-37
ip helper address .................................................... 25-39
ip helper vlan address ............................................. 25-41
ip helper standard .................................................. 25-43
ip helper per-vlan-only .......................................... 25-44
show ip helper ......................................................... 25-46
show ip helper statistics ........................................ 25-48
no ip helper statistics ............................................. 25-50
ip udp relay port ..................................................... 25-52
ip udp relay service ............................................... 25-54
ip udp relay vlan .................................................... 25-56
ip udp relay svc ....................................................... 25-58
ip udp relay address .............................................. 25-60
show ip udp relay .................................................... 25-62
show ip udp relay statistics ................................. 25-64
ip udp relay no statistics ........................................ 25-66
ipv6 udp relay port .................................................. 25-67
ipv6 udp relay service ............................................ 25-69
ipv6 udp relay vlan ................................................ 25-71
ipv6 udp relay svc ................................................. 25-73
ipv6 udp relay address .......................................... 25-75
show ipv6 udp relay ................................................ 25-77
show ipv6 udp relay statistics ............................ 25-79
ipv6 udp relay clear statistics ............................ 25-81
ipv6 dhcp relay admin-state ................................. 25-82
ipv6 dhcp relay interface admin-state .................. 25-84
ipv6 dhcp relay destination ................................. 25-86
ipv6 dhcp relay maximum-hops ......................... 25-88
show ipv6 dhcp relay ............................................ 25-90
dhcp-server .......................................................... 25-92
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcp-server restart</td>
<td>25-94</td>
</tr>
<tr>
<td>show dhcp-server leases</td>
<td>25-95</td>
</tr>
<tr>
<td>show dhcp-server statistics</td>
<td>25-97</td>
</tr>
<tr>
<td>clear dhcp-server statistics</td>
<td>25-105</td>
</tr>
<tr>
<td>dhcpv6-server</td>
<td>25-106</td>
</tr>
<tr>
<td>dhcpv6-server restart</td>
<td>25-108</td>
</tr>
<tr>
<td>show dhcpv6-server leases</td>
<td>25-109</td>
</tr>
<tr>
<td>show dhcpv6-server statistics</td>
<td>25-111</td>
</tr>
<tr>
<td>clear dhcpv6-server statistics</td>
<td>25-121</td>
</tr>
<tr>
<td>dhcp-message-service</td>
<td>25-122</td>
</tr>
<tr>
<td>dhcp-message-service restart</td>
<td>25-123</td>
</tr>
<tr>
<td>show message-service status</td>
<td>25-124</td>
</tr>
<tr>
<td>active-lease-service</td>
<td>25-125</td>
</tr>
<tr>
<td>active-lease-service restart</td>
<td>25-126</td>
</tr>
<tr>
<td>show active-lease-service status</td>
<td>25-127</td>
</tr>
<tr>
<td>dhcp-snooping admin-state</td>
<td>25-128</td>
</tr>
<tr>
<td>dhcp-snooping mac-address-verification</td>
<td>25-130</td>
</tr>
<tr>
<td>dhcp-snooping option-82-data-insertion</td>
<td>25-132</td>
</tr>
<tr>
<td>dhcp-snooping bypass option-82-check</td>
<td>25-134</td>
</tr>
<tr>
<td>dhcp-snooping option-82 format</td>
<td>25-136</td>
</tr>
<tr>
<td>dhcp-snooping option-82 policy</td>
<td>25-139</td>
</tr>
<tr>
<td>dhcp-snooping vlan</td>
<td>25-140</td>
</tr>
<tr>
<td>dhcp-snooping port</td>
<td>25-142</td>
</tr>
<tr>
<td>dhcp-snooping linkagg</td>
<td>25-144</td>
</tr>
<tr>
<td>dhcp-snooping ip-source-filter admin-state</td>
<td>25-146</td>
</tr>
<tr>
<td>dhcp-snooping ip-source-filter</td>
<td>25-148</td>
</tr>
<tr>
<td>dhcp-snooping binding admin-state</td>
<td>25-150</td>
</tr>
<tr>
<td>dhcp-snooping binding timeout</td>
<td>25-152</td>
</tr>
<tr>
<td>dhcp-snooping binding action</td>
<td>25-154</td>
</tr>
<tr>
<td>dhcp-snooping binding persistency</td>
<td>25-156</td>
</tr>
<tr>
<td>dhcp-snooping binding</td>
<td>25-158</td>
</tr>
<tr>
<td>show dhcp-snooping</td>
<td>25-160</td>
</tr>
<tr>
<td>show dhcp-snooping ip-source-filter</td>
<td>25-163</td>
</tr>
<tr>
<td>show dhcp-snooping vlan</td>
<td>25-165</td>
</tr>
<tr>
<td>show dhcp-snooping port</td>
<td>25-167</td>
</tr>
<tr>
<td>dhcp-snooping clear violation-counters</td>
<td>25-169</td>
</tr>
<tr>
<td>show dhcp-snooping counters</td>
<td>25-171</td>
</tr>
<tr>
<td>dhcp-snooping clear counters</td>
<td>25-173</td>
</tr>
<tr>
<td>show dhcp-snooping isf-statistics</td>
<td>25-174</td>
</tr>
<tr>
<td>dhcp-snooping clear isf-statistics</td>
<td>25-176</td>
</tr>
<tr>
<td>show dhcp-snooping binding</td>
<td>25-177</td>
</tr>
<tr>
<td>dhcpv6-snooping vlan admin-state</td>
<td>25-180</td>
</tr>
<tr>
<td>dhcpv6-snooping global admin-state</td>
<td>25-182</td>
</tr>
<tr>
<td>dhcpv6-snooping binding</td>
<td>25-184</td>
</tr>
<tr>
<td>dhcpv6-snooping binding timeout</td>
<td>25-186</td>
</tr>
<tr>
<td>dhcpv6-snooping binding action</td>
<td>25-187</td>
</tr>
<tr>
<td>dhcpv6-snooping binding persistency</td>
<td>25-189</td>
</tr>
<tr>
<td>dhcpv6-snooping ipv6-source-filter</td>
<td>25-191</td>
</tr>
<tr>
<td>ipv6 dhcp guard</td>
<td>25-193</td>
</tr>
<tr>
<td>ipv6 dhcp guard trusted</td>
<td>25-195</td>
</tr>
<tr>
<td>show dhcpv6-snooping</td>
<td>25-197</td>
</tr>
<tr>
<td>show dhcpv6-snooping interfaces</td>
<td>25-199</td>
</tr>
</tbody>
</table>
# Chapter 26  VRRP Commands

- show ipv6 dhcp guard ........................................................................... 25-205
- show dhcpv6-snooping ipv6-source-filter ............................................. 25-203
- show ipv6 dhcp guard ........................................................................... 25-205

## Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vrrp track-association</td>
<td>26-52</td>
</tr>
<tr>
<td>show vrrp track</td>
<td>26-50</td>
</tr>
<tr>
<td>show vrrp statistics</td>
<td>26-46</td>
</tr>
<tr>
<td>show vrrp track-association</td>
<td>26-52</td>
</tr>
<tr>
<td>show vrrp group</td>
<td>26-55</td>
</tr>
<tr>
<td>show vrrp group-association</td>
<td>26-57</td>
</tr>
</tbody>
</table>

# Chapter 27  OSPF Commands

- ip load ospf ................................................................. 27-1
- ip ospf admin-state ................................................... 27-3
- ip ospf asbr ............................................................... 27-4
- ip ospf exit-overflow-interval ....................... 27-5
- ip ospf extlsdb-limit .................................................. 27-6
- ip ospf host ............................................................... 27-7
- ip ospf mtu-checking ................................................... 27-8
- ip ospf default-originate ......................................... 27-9
- ip ospf route-tag ........................................................ 27-10
- ip ospf spf-timer ......................................................... 27-11
- ip ospf virtual-link ..................................................... 27-12
- ip ospf neighbor .......................................................... 27-13
- ip ospf redist-bgp-internal ....................................... 27-14
- ip ospf area ............................................................... 27-15
- ip ospf area default-metric ................................. 27-16
- ip ospf area range ........................................................ 27-17
- ip ospf interface ........................................................ 27-18
- ip ospf interface admin-state ................................. 27-19
- ip ospf interface area ..................................................... 27-20
- ip ospf interface auth-key .......................................... 27-21
- ip ospf interface auth-type .............................................. 27-22
- ip ospf interface dead-interval .............................. 27-23

- show vrrp group-association ...................................... 26-57
Chapter 28 OSPFv3 Commands

ipv6 ospf spf-timer ........................................... 28-10
ipv6 ospf virtual-link ........................................ 28-12
ipv6 ospf area .................................................. 28-14
ipv6 ospf area area-summary ............................ 28-16
ipv6 ospf area nssa-translator-role ................ 28-18
ipv6 ospf area nssa-translator-stab-interval .... 28-20
ipv6 ospf area nssa-summary ............................ 28-21
ipv6 ospf interface ........................................... 28-22
ipv6 ospf interface admin-state ......................... 28-23
ipv6 ospf interface suppress-link-lsa ............. 28-25
ipv6 ospf interface type ................................... 28-26
Chapter 29 IS-IS Commands

*ip load isis* .................................................................................................................. 29-4
*ip isis admin-state* ........................................................................................................ 29-5
*ip isis area-id* ................................................................................................................ 29-6
*ip isis level-capability* .................................................................................................... 29-8
*ip isis auth-check* ........................................................................................................... 29-10
*ip isis auth-type* ............................................................................................................ 29-12
*ip isis csnp-auth* ............................................................................................................ 29-14
*ip isis hello-auth* ............................................................................................................ 29-15
*ip isis psnp-auth* ............................................................................................................ 29-16
*ip isis lsp-lifetime* ........................................................................................................ 29-17
*ip isis lsp-wait* ................................................................................................................ 29-19
*ip isis spf-wait* .............................................................................................................. 29-21
*ip isis summary-address* ............................................................................................... 29-23
*ip isis overload* .............................................................................................................. 29-25
*ip isis overload-on-boot* ............................................................................................... 29-27
*ip isis graceful-restart* .................................................................................................... 29-29
*ip isis graceful-restart helper* ...................................................................................... 29-31
*ip isis strict-adjacency-check* ...................................................................................... 29-33
*ip isis level auth-type* .................................................................................................... 29-34
*ip isis level hello-auth* .................................................................................................. 29-36
*ip isis level csnp-auth* .................................................................................................. 29-38
*ip isis level psnp-auth* .................................................................................................. 29-40
Contents

- ip isis level wide-metrics-only ................................................................. 29-42
- ip isis activate-ipv6|ipv4 ................................................................. 29-44
- ip isis vlan ......................................................................................... 29-45
- ip isis vlan admin-state ................................................................. 29-47
- ip isis vlan interface-type ................................................................. 29-49
- ip isis vlan csnp-interval ................................................................. 29-51
- ip isis vlan hello-auth-type ............................................................. 29-53
- ip isis vlan level-capability .............................................................. 29-55
- ip isis vlan lsp-pacing-interval ......................................................... 29-57
- ip isis vlan passive ........................................................................... 29-59
- ip isis vlan retransmit-interval ......................................................... 29-61
- ip isis vlan default-type ................................................................. 29-63
- ip isis vlan level hello-auth-type ...................................................... 29-64
- ip isis vlan level hello-interval ......................................................... 29-66
- ip isis vlan level hello-multiplier ...................................................... 29-68
- ip isis vlan level metric ................................................................. 29-70
- ip isis vlan level passive ................................................................. 29-72
- ip isis vlan level priority ................................................................. 29-74
- ip isis summary-address6 ............................................................... 29-76
- ip isis bfd-state .............................................................................. 29-78
- ip isis bfd-state all-vlans ................................................................. 29-80
- ip isis vlan bfd-state ........................................................................ 29-81
- show ip isis adjacency ..................................................................... 29-83
- show ip isis database ........................................................................ 29-87
- show ip isis hostname ...................................................................... 29-92
- show ip isis routes ........................................................................... 29-94
- show ip isis routes6 .......................................................................... 29-96
- show ip isis spf ................................................................................ 29-98
- show ip isis spf-log .......................................................................... 29-100
- show ip isis statistics ....................................................................... 29-102
- show ip isis status ............................................................................ 29-105
- show ip isis summary-address ........................................................... 29-109
- show ip isis vlan ............................................................................. 29-111
- show ip isis summary-address6 .......................................................... 29-115
- clear ip isis adjacency ..................................................................... 29-117
- clear ip isis lsp-database .................................................................. 29-119
- clear ip isis spf-log .......................................................................... 29-121
- clear ip isis statistics ....................................................................... 29-122
- ip isis multi-topology ...................................................................... 29-124

Chapter 30 BGP Commands ........................................................................... 30-1
- ip load bgp ...................................................................................... 30-6
- ip bgp admin-state ........................................................................... 30-8
- ip bgp autonomous-system .............................................................. 30-10
- ip bgp bestpath as-path ignore ......................................................... 30-12
- ip bgp cluster-id ............................................................................ 30-14
- ip bgp default local-preference ......................................................... 30-16
- ip bgp fast-external-failover ............................................................ 30-18
- ip bgp always-compare-med ............................................................ 30-20
- ip bgp bestpath med missing-as-worst ............................................. 30-22
- ip bgp client-to-client reflection ...................................................... 30-24
- ip bgp as-origin-interval ................................................................. 30-26
Contents

ip bgp synchronization ............................................................... 30-28
ip bgp confederation identifier .................................................. 30-30
ip bgp maximum-paths ............................................................... 30-32
ip bgp log-neighbor-changes .................................................... 30-34
ip bgp dampening ................................................................... 30-35
ip bgp dampening clear .............................................................. 30-38
ip bgp as-format ....................................................................... 30-39
ip bgp aggregate-address .......................................................... 30-40
ip bgp aggregate-address admin-state ....................................... 30-42
ip bgp aggregate-address as-set ................................................. 30-44
ip bgp aggregate-address community ........................................ 30-46
ip bgp aggregate-address local-preference ................................. 30-48
ip bgp aggregate-address metric ................................................. 30-50
ip bgp aggregate-address summary-only .................................... 30-52
ip bgp network .......................................................................... 30-54
ip bgp network admin-state ...................................................... 30-56
ip bgp network community ........................................................ 30-58
ip bgp network local-preference ................................................. 30-60
ip bgp network metric ............................................................... 30-62
ip bgp neighbor ................................................................. 30-64
ip bgp neighbor ttl-security ..................................................... 30-66
ip bgp neighbor default-origin .................................................. 30-68
ip bgp neighbor admin-state ..................................................... 30-70
ip bgp neighbor advertisement-interval ..................................... 30-72
ip bgp neighbor clear ............................................................... 30-74
ip bgp neighbor route-reflector-client ....................................... 30-76
ip bgp neighbor activate-ip4 ...................................................... 30-78
ip bgp neighbor timers ............................................................. 30-80
ip bgp neighbor conn-retry-interval .......................................... 30-82
ip bgp neighbor auto-restart ...................................................... 30-84
ip bgp neighbor maximum-prefix ............................................. 30-86
ip bgp neighbor md5 key ........................................................... 30-88
ip bgp neighbor ebgp-multihop ............................................... 30-90
ip bgp neighbor description ..................................................... 30-92
ip bgp neighbor next-hop-self .................................................. 30-94
ip bgp neighbor passive ........................................................... 30-96
ip bgp neighbor remote-as ....................................................... 30-98
ip bgp neighbor remove-private-as ........................................... 30-100
ip bgp neighbor soft-reconfiguration ....................................... 30-102
ip bgp neighbor stats-clear ....................................................... 30-104
ip bgp confederation neighbor .................................................. 30-105
ip bgp neighbor update-source ................................................ 30-107
ip bgp neighbor in-aspathlist .................................................... 30-109
ip bgp neighbor in-communitylist ............................................. 30-111
ip bgp neighbor in-prefixlist ..................................................... 30-113
ip bgp neighbor in-prefix6list ................................................... 30-115
ip bgp neighbor out-aspathlist ................................................. 30-117
ip bgp neighbor out-communitylist .......................................... 30-119
ip bgp neighbor out-prefixlist ................................................... 30-121
ip bgp neighbor out-prefix6list .................................................. 30-123
ip bgp neighbor route-map ....................................................... 30-125
ip bgp neighbor clear soft ....................................................... 30-127
ipv6 bgp neighbor advertisement-interval ..........................................................30-305
ipv6 bgp neighbor ipv4-nexthop ........................................................................30-304
ipv6 bgp neighbor update-source .......................................................................30-302
ipv6 bgp neighbor passive ..................................................................................30-313
ipv6 bgp neighbor default-originate ...................................................................30-300
ipv6 bgp neighbor route-reflector-client ............................................................30-342
ipv6 bgp neighbor clear soft ...............................................................................30-340
ipv6 bgp neighbor route-map ............................................................................30-338
ipv6 bgp neighbor out-prefix6list .......................................................................30-336
ipv6 bgp neighbor out-prefixlist .........................................................................30-334
ipv6 bgp neighbor out-communitylist ................................................................30-332
ipv6 bgp neighbor out-aspathlist ........................................................................30-330
ipv6 bgp neighbor in-prefix6list .........................................................................30-328
ipv6 bgp neighbor in-prefixlist ...........................................................................30-326
ipv6 bgp neighbor in-communitylist ...... ............................................................30-324
ipv6 bgp neighbor in-aspathlist ..........................................................................30-322
ipv6 bgp neighbor unicast ........................................................................................30-275
ipv6 bgp neighbor ttl-security ............................................................................30-277
ipv6 bgp neighbor activate-ipv6 .........................................................................30-279
ipv6 bgp neighbor activate-ipv4 .........................................................................30-279
ipv6 bgp neighbor activate-ipv6 .........................................................................30-281
ipv6 bgp neighbor activate-ipv4 .........................................................................30-282
ipv6 bgp neighbor admin-state ...........................................................................30-275
ipv6 bgp neighbor admin-state ...........................................................................30-284
ipv6 bgp neighbor clear ......................................................................................30-286
ipv6 bgp neighbor auto-restart ...........................................................................30-288
ipv6 bgp neighbor remote-as ..............................................................................30-290
ipv6 bgp neighbor timers ....................................................................................30-292
ipv6 bgp neighbor maximum-prefix ..................................................................30-294
ipv6 bgp neighbor next-hop-self .........................................................................30-296
ipv6 bgp neighbor conn-retry-interval ...............................................................30-298
ipv6 bgp neighbor default-originate .................................................................30-300
ipv6 bgp neighbor update-source .......................................................................30-302
ipv6 bgp neighbor ipv4-nexthop .........................................................................30-304
ipv6 bgp neighbor advertisement-interval ..........................................................30-305
ipv6 bgp neighbor description ............................................................................30-307
ipv6 bgp neighbor ebgp-multihop ......................................................................30-309
ipv6 bgp neighbor update-source-address ...........................................................30-311
ipv6 bgp neighbor passive ..................................................................................30-313
ipv6 bgp neighbor remove-private-as ..................................................................30-315
ipv6 bgp neighbor soft-reconfiguration ..............................................................30-317
ipv6 bgp neighbor stats-clear ...........................................................................30-319
ip bgp confederation neighbor6 ...........................................................................30-320
ipv6 bgp neighbor in-aspathlist .........................................................................30-322
ipv6 bgp neighbor in-communitylist ..................................................................30-324
ipv6 bgp neighbor in-prefixlist ...........................................................................30-326
ipv6 bgp neighbor in-prefix6list .........................................................................30-328
ipv6 bgp neighbor out-aspathlist .........................................................................30-330
ipv6 bgp neighbor out-communitylist ................................................................30-332
ipv6 bgp neighbor out-prefixlist .........................................................................30-334
ipv6 bgp neighbor out-prefix6list .......................................................................30-336
ipv6 bgp neighbor route-map ............................................................................30-338
ipv6 bgp neighbor clear soft ...............................................................................30-340
ipv6 bgp neighbor route-reflector-client ............................................................30-342
show ip bgp policy prefix6-list ...........................................................................30-243
show ip bgp policy route-map .............................................................................30-245
ip bgp graceful-restart .......................................................................................30-248
ip bgp graceful-restart restart-interval ...............................................................30-250
ip bgp unicast ......................................................................................................30-251
ip bgp unicast ......................................................................................................30-253
ip bgp neighbor activate-ipv6 .............................................................................30-254
ip bgp neighbor activate-ipv4 .............................................................................30-254
show ipv6 bgp path ..............................................................................................30-257
show ipv6 bgp routes ...........................................................................................30-261
ipv6 bgp network .................................................................................................30-263
ipv6 bgp network community ............................................................................30-265
ipv6 bgp network local-preference ....................................................................30-267
ipv6 bgp network metric ...................................................................................30-269
ipv6 bgp network admin-state ...........................................................................30-271
show ipv6 bgp network ........................................................................................30-273
ipv6 bgp neighbor ...............................................................................................30-275
ipv6 bgp neighbor ttl-security ............................................................................30-277
ipv6 bgp neighbor activate-ipv4 .........................................................................30-279
Chapter 31  Server Load Balancing Commands ................................................................. 31-1
  ip slb admin-state ........................................................................................................ 31-2
  ip slb reset statistics ................................................................................................ 31-4
  ip slb cluster ................................................................................................................ 31-5
  ip slb cluster admin-state ........................................................................................... 31-7
  ip slb cluster ping period .......................................................................................... 31-9
  ip slb cluster ping timeout ....................................................................................... 31-11
  ip slb cluster ping retries ........................................................................................ 31-13
  ip slb cluster probe ................................................................................................... 31-15
  ip slb server ip cluster ............................................................................................. 31-17
  ip slb server ip cluster probe .................................................................................. 31-19
  ip slb probe ............................................................................................................... 31-21
  ip slb probe timeout .................................................................................................. 31-23
  ip slb probe period .................................................................................................... 31-25
  ip slb probe port ......................................................................................................... 31-27
  ip slb probe retries .................................................................................................... 31-29
  ip slb probe username .............................................................................................. 31-31
  ip slb probe password ............................................................................................. 31-33
  ip slb probe url ......................................................................................................... 31-35
  ip slb probe status .................................................................................................... 31-37
  ip slb probe send ....................................................................................................... 31-39
  ip slb probe expect .................................................................................................... 31-41
  show ip slb ............................................................................................................... 31-43
  show ip slb clusters ................................................................................................. 31-45
  show ip slb cluster ................................................................................................. 31-48
  show ip slb cluster server ...................................................................................... 31-52
  show ip slb servers ................................................................................................. 31-55
  show ip slb probe ................................................................................................. 31-57

Chapter 32  IP Multicast Switching Commands ............................................................. 32-1
  ip multicast admin-state ........................................................................................ 32-3
  ip multicast flood-unknown ................................................................................... 32-5
  ip multicast version ................................................................................................. 32-8
  ip multicast port max-group .................................................................................. 32-10
  ip multicast max-group ......................................................................................... 32-12
  ip multicast static-neighbor .................................................................................. 32-15
  ip multicast static-querier .................................................................................... 32-17
  ip multicast static-group ....................................................................................... 32-19
  ip multicast query-interval .................................................................................... 32-21
  ip multicast last-member-query-interval ................................................................. 32-23
  ip multicast query-response-interval ...................................................................... 32-25
  ip multicast unsolicited-report-interval ............................................................... 32-27
  ip multicast router-timeout .................................................................................... 32-29
  ip multicast source-timeout ................................................................................... 32-31
  ip multicast querying .............................................................................................. 32-33
  ip multicast robustness ......................................................................................... 32-35
Chapter 33  DVMRP Commands

ip load dvmrp ................................................................. 33-2
ip dvmrp admin-state ...................................................... 33-3
ip dvmrp flash-interval .................................................... 33-5
ip dvmrp graft-timeout .................................................... 33-6
ip dvmrp interface .......................................................... 33-7
ip dvmrp interface metric .................................................. 33-9
ip dvmrp interface mbr-default-information ......................... 33-11
ip dvmrp neighbor-interval ............................................... 33-13
ip dvmrp neighbor-timeout ................................................. 33-14
ip dvmrp prune-lifetime .................................................... 33-15
ip dvmrp prune-timeout ...................................................... 33-17
ip dvmrp report-interval .................................................... 33-19
ip dvmrp route-holddown .................................................. 33-20
ip dvmrp route-timeout ...................................................... 33-22
ip dvmrp subord-default ................................................... 33-24
show ip dvmrp ................................................................. 33-26
Chapter 34  PIM Commands

Contents

show ip dvmrp interface ................................................................. 33-30
show ip dvmrp neighbor ............................................................... 33-33
show ip dvmrp nexthop ................................................................. 33-35
show ip dvmrp prune ................................................................. 33-37
show ip dvmrp route ................................................................. 33-39
show ip dvmrp tunnel ............................................................... 33-41

show ip pim sparse-admin-state .................................................. 34-3
ip load pim ................................................................................. 34-4
ip pim sparse-admin-state ........................................................ 34-5
ip pim bidir-admin-state ............................................................ 34-7
ip pim dense-admin-state ......................................................... 34-9
ip pim rp-hash-admin-state ....................................................... 34-11
ip pim ssm-group ....................................................................... 34-13
ip pim dense-group ................................................................. 34-15
ip pim cbmr .............................................................................. 34-17
ip pim static-rp ........................................................................... 34-19
ip pim anycast-rp ....................................................................... 34-21
ip pim candidate-rp .................................................................... 34-23
ip pim rp-threshold ................................................................... 34-25
ip pim keepalive-period ............................................................ 34-27
ip pim max-rps ........................................................................... 34-29
ip pim probe-time ..................................................................... 34-31
ip pim register checksum .......................................................... 34-33
ip pim register-packing ............................................................ 34-35
ip pim register-mtu ..................................................................... 34-37
ip pim register-delay ............................................................... 34-39
ip pim register-suppress-timeout ............................................... 34-41
ip pim register-rate-limit .......................................................... 34-43
ip pim spt-admin-state ............................................................. 34-45
ip pim state-refresh-interval ..................................................... 34-47
ip pim state-refresh-limit .......................................................... 34-49
ip pim state-refresh-ttl .............................................................. 34-51
ip pim interface ......................................................................... 34-53
ip pim neighbor-loss-notification-period .................................... 34-55
ip pim invalid-register-notification-period .................................. 34-57
ip pim invalid-join-prune-notification-period ................................ 34-59
ip pim rp-mapping-notification-period ....................................... 34-61
ip pim interface-election-notification-period ................................ 34-63
ip pim nonbidir-hello-notification-period .................................... 34-65
ip pim df-abort ........................................................................... 34-67
ip pim mbr all-sources ............................................................ 34-69
ip pim df-periodic-interval ......................................................... 34-71
ip pim bfd-state ......................................................................... 34-73
ip pim bfd-state all-interfaces ................................................... 34-75
ip pim interface bfd-state ......................................................... 34-77
ip pim bidir ssm-compat ............................................................ 34-78
ip pim bidir fast-join ............................................................... 34-80
ip pim sparse asm-fast-join ....................................................... 34-82
ip pim sparse ssm-fast-join ......................................................... 34-83
ip pim join-prune-packing ........................................................ 34-84
show ip pim sparse ............................................................... 34-86
Contents

show ip pim dense .............................................................. 34-92
show ip pim ssm group ........................................................... 34-95
show ip pim dense group ....................................................... 34-97
show ip pim neighbor ........................................................ 34-99
show ip pim candidate-rp ................................................... 34-102
show ip pim group-map ....................................................... 34-104
show ip pim interface ......................................................... 34-107
show ip pim static-rp .......................................................... 34-111
show ip pim anycast-rp ....................................................... 34-113
show ip pim cbsr ............................................................... 34-115
show ip pim bsr ................................................................. 34-117
show ip pim notifications ................................................... 34-119
show ip pim groute ............................................................. 34-122
show ip pim sgroute .......................................................... 34-126
show ip pim df-election ...................................................... 34-131
ipv6 pim sparse admin-state ............................................. 34-133
ipv6 pim bidir admin-state ............................................... 34-135
ipv6 pim dense admin-state .............................................. 34-137
ipv6 pim ssm group .......................................................... 34-139
ipv6 pim dense group ........................................................ 34-141
ipv6 pim cbsr ................................................................. 34-143
ipv6 pim static-rp ............................................................. 34-145
ipv6 pim anycast-rp .......................................................... 34-147
ipv6 pim candidate-rp ...................................................... 34-149
ipv6 pim rp-switchover ..................................................... 34-151
ipv6 pim register-rate-limit ............................................. 34-153
ipv6 pim register-packing ............................................... 34-155
ipv6 pim register-mtu ....................................................... 34-157
ipv6 pim register-delay .................................................... 34-159
ipv6 pim spf admin-state .................................................. 34-161
ipv6 pim interface ........................................................... 34-163
ipv6 pim bfd-state ........................................................... 34-167
ipv6 pim bfd-state all-interfaces ..................................... 34-169
ipv6 pim interface bfd-state ............................................. 34-170
ipv6 pim bidir ssm-compat ............................................... 34-172
ipv6 pim bidir fast-join .................................................... 34-174
ipv6 pim sparse asm-fast-join ......................................... 34-175
ipv6 pim sparse ssm-fast-join .......................................... 34-177
ipv6 pim joinprune-packing ........................................... 34-178
show ipv6 pim sparse ....................................................... 34-180
show ipv6 pim dense ....................................................... 34-184
show ipv6 pim ssm group .................................................. 34-186
show ipv6 pim dense group ................................................ 34-188
show ipv6 pim interface .................................................... 34-190
show ipv6 pim neighbor ................................................... 34-194
show ipv6 pim static-rp .................................................... 34-198
show ipv6 pim anycast-rp ................................................ 34-200
show ipv6 pim group-map ................................................. 34-202
show ipv6 pim candidate-rp ............................................. 34-204
show ipv6 pim cbsr ......................................................... 34-206
show ipv6 pim bsr .......................................................... 34-208
show ipv6 pim groute ....................................................... 34-210
Chapter 35  Multicast Routing Commands

- show ipv6 pim sgroute ................................................................. 34-214
- show ipv6 pim df-election ............................................................. 34-218

Chapter 36  QoS Commands

- qos ............................................................... 36-1
- qos trust-ports .......................................................... 36-5
- qos forward log .......................................................... 36-7
- qos log console .......................................................... 36-8
- qos log lines ............................................................. 36-10
- qos log level ............................................................. 36-12
- qos stats interval ......................................................... 36-14
- qos phones ............................................................... 36-15
- qos quarantine mac-group .................................................. 36-17
- qos user-port .............................................................. 36-19
- qos dei ........................................................................ 36-22
- debug qos ............................................................... 36-24
- debug qos internal ......................................................... 36-26
- clear qos log ............................................................... 36-28
- qos apply .................................................................. 36-29
- qos revert ................................................................... 36-31
- qos flush .................................................................... 36-33
- qos reset ....................................................................... 36-35
- qos stats reset ........................................................... 36-36
- qos switch-group .......................................................... 36-37
- qos port reset .............................................................. 36-39
- qos port ................................................................. 36-41
- qos port trusted ............................................................. 36-43
- qos port maximum egress-bandwidth .................................. 36-45
- qos port maximum ingress-bandwidth .................................. 36-47
- qos port maximum depth .................................................. 36-49
- qos port default 802.1p .................................................. 36-51
- qos port default dscp ...................................................... 36-53
- qos port default classification ............................................ 36-55
- qos port dei .................................................................. 36-57
- qos qsp import ............................................................. 36-59
- qos qsp qp .................................................................. 36-61
- qos qsi qsp ............................................................... 36-63
## Chapter 37 QoS Policy Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos qsp system-default</td>
<td>36-66</td>
</tr>
<tr>
<td>qos qos stats</td>
<td>36-68</td>
</tr>
<tr>
<td>show qos port</td>
<td>36-70</td>
</tr>
<tr>
<td>show qos slice</td>
<td>36-73</td>
</tr>
<tr>
<td>show qos log</td>
<td>36-75</td>
</tr>
<tr>
<td>show qos config</td>
<td>36-77</td>
</tr>
<tr>
<td>show qos statistics</td>
<td>36-80</td>
</tr>
<tr>
<td>show qos qos i summary</td>
<td>36-83</td>
</tr>
<tr>
<td>show qos qsp</td>
<td>36-85</td>
</tr>
<tr>
<td>show qos wrp</td>
<td>36-90</td>
</tr>
<tr>
<td>show qos qos i</td>
<td>36-93</td>
</tr>
<tr>
<td>show qos qos i stats</td>
<td>36-98</td>
</tr>
<tr>
<td>show qos qos i ecn-stats</td>
<td>36-101</td>
</tr>
<tr>
<td>show qos qos i wred-stats</td>
<td>36-103</td>
</tr>
<tr>
<td>show qos qsp system-default</td>
<td>36-105</td>
</tr>
<tr>
<td>clear qos qos i stats</td>
<td>36-107</td>
</tr>
<tr>
<td>qos qsp dcb import</td>
<td>36-109</td>
</tr>
<tr>
<td>qos qos dcb tc</td>
<td>36-111</td>
</tr>
<tr>
<td>qos qos dcb tc-numbering</td>
<td>36-113</td>
</tr>
<tr>
<td>qos qos qsp dcb</td>
<td>36-115</td>
</tr>
<tr>
<td>qos qos dcb dcbx version</td>
<td>36-117</td>
</tr>
<tr>
<td>qos qos dcb dcbx admin-state</td>
<td>36-119</td>
</tr>
<tr>
<td>qos qos dcb dcbx ets</td>
<td>36-121</td>
</tr>
<tr>
<td>qos qos dcb dcbx pfc</td>
<td>36-123</td>
</tr>
<tr>
<td>show qos qos dcb</td>
<td>36-125</td>
</tr>
<tr>
<td>show qos qos dcb dcbx</td>
<td>36-127</td>
</tr>
<tr>
<td>show qos qos dcb dcbx ets</td>
<td>36-131</td>
</tr>
<tr>
<td>show qos qos dcb dcbx pfc</td>
<td>36-135</td>
</tr>
<tr>
<td>show qos pfc-lossless-usage</td>
<td>36-138</td>
</tr>
<tr>
<td>show qos qos dcb pfc stats</td>
<td>36-140</td>
</tr>
<tr>
<td>clear qos qos dcb pfc stats</td>
<td>36-142</td>
</tr>
<tr>
<td>qos ecnp import ecnp</td>
<td>36-143</td>
</tr>
<tr>
<td>qos ecnp value</td>
<td>36-145</td>
</tr>
<tr>
<td>qos qos ecnp</td>
<td>36-147</td>
</tr>
<tr>
<td>qos qos qsp ecn</td>
<td>36-149</td>
</tr>
<tr>
<td>show qos qos ecnp</td>
<td>36-151</td>
</tr>
</tbody>
</table>

**Policy Rule**

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy rule</td>
<td>37-4</td>
</tr>
<tr>
<td>iec message-type priority</td>
<td>37-8</td>
</tr>
<tr>
<td>iec message-type flush</td>
<td>37-11</td>
</tr>
<tr>
<td>iec show</td>
<td>37-12</td>
</tr>
<tr>
<td>policy validity-period</td>
<td>37-13</td>
</tr>
<tr>
<td>policy list</td>
<td>37-16</td>
</tr>
<tr>
<td>policy list rules</td>
<td>37-18</td>
</tr>
<tr>
<td>policy network group</td>
<td>37-21</td>
</tr>
<tr>
<td>policy service group</td>
<td>37-23</td>
</tr>
<tr>
<td>policy mac group</td>
<td>37-25</td>
</tr>
<tr>
<td>policy port group</td>
<td>37-27</td>
</tr>
<tr>
<td>policy map group</td>
<td>37-30</td>
</tr>
<tr>
<td>policy service</td>
<td>37-32</td>
</tr>
<tr>
<td>policy service protocol</td>
<td>37-35</td>
</tr>
<tr>
<td>Policy Condition</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>policy condition vxlan</td>
<td>37-136</td>
</tr>
<tr>
<td>policy condition destination vlan</td>
<td>37-112</td>
</tr>
<tr>
<td>policy condition vxlan inner source mac-group</td>
<td>37-141</td>
</tr>
<tr>
<td>policy condition vxlan inner source mac</td>
<td>37-139</td>
</tr>
<tr>
<td>policy condition appfp-group</td>
<td>37-134</td>
</tr>
<tr>
<td>policy condition app-mon-application-name</td>
<td>37-132</td>
</tr>
<tr>
<td>policy condition app-mon-application-group</td>
<td>37-130</td>
</tr>
<tr>
<td>policy condition fragments</td>
<td>37-128</td>
</tr>
<tr>
<td>policy condition destination port</td>
<td>37-120</td>
</tr>
<tr>
<td>policy condition source port</td>
<td>37-118</td>
</tr>
<tr>
<td>policy condition inner 802.1p</td>
<td>37-116</td>
</tr>
<tr>
<td>policy condition 802.1p</td>
<td>37-114</td>
</tr>
<tr>
<td>policy condition source mac group</td>
<td>37-104</td>
</tr>
<tr>
<td>policy condition destination mac</td>
<td>37-102</td>
</tr>
<tr>
<td>policy condition source mac</td>
<td>37-100</td>
</tr>
<tr>
<td>policy condition dscp</td>
<td>37-98</td>
</tr>
<tr>
<td>policy condition source mac-group</td>
<td>37-106</td>
</tr>
<tr>
<td>policy condition destination mac-group</td>
<td>37-104</td>
</tr>
<tr>
<td>policy condition destination ip</td>
<td>37-52</td>
</tr>
<tr>
<td>policy condition destination ipv6</td>
<td>37-54</td>
</tr>
<tr>
<td>policy condition multicast ip</td>
<td>37-56</td>
</tr>
<tr>
<td>policy condition source network group</td>
<td>37-58</td>
</tr>
<tr>
<td>policy condition destination network group</td>
<td>37-60</td>
</tr>
<tr>
<td>policy condition multicast network group</td>
<td>37-62</td>
</tr>
<tr>
<td>policy condition source ip-port</td>
<td>37-64</td>
</tr>
<tr>
<td>policy condition destination ip-port</td>
<td>37-66</td>
</tr>
<tr>
<td>policy condition tcp-port</td>
<td>37-68</td>
</tr>
<tr>
<td>policy condition destination tcp-port</td>
<td>37-70</td>
</tr>
<tr>
<td>policy condition source udp-port</td>
<td>37-72</td>
</tr>
<tr>
<td>policy condition destination udp-port</td>
<td>37-74</td>
</tr>
<tr>
<td>policy condition ethertype</td>
<td>37-76</td>
</tr>
<tr>
<td>policy condition established</td>
<td>37-78</td>
</tr>
<tr>
<td>policy condition tcpflags</td>
<td>37-80</td>
</tr>
<tr>
<td>policy condition service</td>
<td>37-82</td>
</tr>
<tr>
<td>policy condition service group</td>
<td>37-84</td>
</tr>
<tr>
<td>policy condition icmp-type</td>
<td>37-86</td>
</tr>
<tr>
<td>policy condition icmpcode</td>
<td>37-88</td>
</tr>
<tr>
<td>policy condition ip-protocol</td>
<td>37-90</td>
</tr>
<tr>
<td>policy condition ipv6</td>
<td>37-92</td>
</tr>
<tr>
<td>policy condition flow-label</td>
<td>37-94</td>
</tr>
<tr>
<td>policy condition tos</td>
<td>37-96</td>
</tr>
<tr>
<td>policy condition dscp</td>
<td>37-98</td>
</tr>
<tr>
<td>policy condition source mac</td>
<td>37-106</td>
</tr>
<tr>
<td>policy condition destination mac-group</td>
<td>37-104</td>
</tr>
<tr>
<td>policy condition source mac-group</td>
<td>37-102</td>
</tr>
<tr>
<td>policy condition destination mac-group</td>
<td>37-100</td>
</tr>
<tr>
<td>policy condition source vlan</td>
<td>37-108</td>
</tr>
<tr>
<td>policy condition inner source-vlan</td>
<td>37-110</td>
</tr>
<tr>
<td>policy condition destination vlan</td>
<td>37-112</td>
</tr>
<tr>
<td>policy condition 802.1p</td>
<td>37-114</td>
</tr>
<tr>
<td>policy condition inner 802.1p</td>
<td>37-116</td>
</tr>
<tr>
<td>policy condition source port</td>
<td>37-118</td>
</tr>
<tr>
<td>policy condition destination port</td>
<td>37-120</td>
</tr>
<tr>
<td>policy condition source port-group</td>
<td>37-122</td>
</tr>
<tr>
<td>policy condition destination port-group</td>
<td>37-124</td>
</tr>
<tr>
<td>policy condition vrf</td>
<td>37-126</td>
</tr>
<tr>
<td>policy condition fragments</td>
<td>37-128</td>
</tr>
<tr>
<td>policy condition app-mon-application-group</td>
<td>37-130</td>
</tr>
<tr>
<td>policy condition app-mon-application-name</td>
<td>37-132</td>
</tr>
<tr>
<td>policy condition appfp-group</td>
<td>37-134</td>
</tr>
<tr>
<td>policy condition vxlan</td>
<td>37-136</td>
</tr>
<tr>
<td>policy condition vxlan inner source mac</td>
<td>37-139</td>
</tr>
<tr>
<td>policy condition vxlan inner source mac-group</td>
<td>37-141</td>
</tr>
</tbody>
</table>
## Chapter 38 Policy Server Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy server load</td>
<td>38-2</td>
</tr>
<tr>
<td>policy server flush</td>
<td>38-3</td>
</tr>
<tr>
<td>policy server</td>
<td>38-4</td>
</tr>
<tr>
<td>show policy server</td>
<td>38-6</td>
</tr>
<tr>
<td>show policy server long</td>
<td>38-8</td>
</tr>
<tr>
<td>show policy server statistics</td>
<td>38-10</td>
</tr>
<tr>
<td>show policy server rules</td>
<td>38-12</td>
</tr>
<tr>
<td>show policy server events</td>
<td>38-14</td>
</tr>
</tbody>
</table>

## Chapter 39 AAA Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa radius-server</td>
<td>39-1</td>
</tr>
</tbody>
</table>

---

**Contents**

- show policy ipv6-summary .................................................. 37-222
- show policy ipv4-summary .................................................. 37-220
- show policy list ..................................................................... 37-218
- show active policy list ....................................................... 37-216
- show policy validity period .................................................. 37-214
- show policy rule .................................................................. 37-212
- show active policy rule ....................................................... 37-210
- show policy condition ......................................................... 37-207
- show policy map group ......................................................... 37-203
- show policy port group ......................................................... 37-201
- show policy map group ......................................................... 37-203
- show policy action ............................................................. 37-205
- show policy condition ......................................................... 37-207
- show active policy rule ....................................................... 37-210
- show policy rule .................................................................. 37-212
- show policy validity period .................................................. 37-214
- show active policy list ....................................................... 37-216
- show policy list ................................................................. 37-218
- show policy ipv4-summary .................................................. 37-220
- show policy ipv6-summary .................................................. 37-222

- policy condition vxlan inner source ip .................................. 37-143
- policy condition vxlan inner source ipv6 ................................ 37-145
- policy condition vxlan inner ip-protocol ............................... 37-147
- policy condition vxlan inner l4-port ..................................... 37-149
- policy condition vxlan vxlan-port ......................................... 37-151
- policy action ....................................................................... 37-153
- policy action disposition ..................................................... 37-156
- policy action shared ............................................................ 37-158
- policy action priority .......................................................... 37-160
- policy action maximum bandwidth ...................................... 37-162
- policy action maximum depth ............................................. 37-164
- policy action cir .................................................................. 37-166
- policy action cpu priority .................................................... 37-169
- policy action tos ................................................................. 37-171
- policy action 802.1p ............................................................ 37-173
- policy action dscp ............................................................... 37-175
- policy action map ............................................................... 37-177
- policy action permanent gateway-ip ..................................... 37-179
- policy action permanent gateway-ipv6 ............................... 37-181
- policy action port-disable .................................................... 37-183
- policy action redirect port ................................................... 37-185
- policy action redirect linkagg .............................................. 37-187
- policy action no-cache ....................................................... 37-189
- policy action mirror ........................................................... 37-191
- show policy network group .................................................. 37-193
- show policy service ............................................................ 37-195
- show policy service group .................................................. 37-197
- show policy mac group ....................................................... 37-199
- show policy port group ....................................................... 37-201
- show policy map group ....................................................... 37-203
- show policy action ............................................................. 37-205
- show policy condition ......................................................... 37-207
- show active policy rule ....................................................... 37-210
- show policy rule .................................................................. 37-212
- show policy validity period .................................................. 37-214
- show active policy list ....................................................... 37-216
- show policy list ................................................................. 37-218
- show policy ipv4-summary .................................................. 37-220
- show policy ipv6-summary .................................................. 37-222

---

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  xxxvi
### Contents

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa radius-server health-check</td>
<td>39-7</td>
</tr>
<tr>
<td>aaa radius unp-profile-precedence</td>
<td>39-9</td>
</tr>
<tr>
<td>aaa test-radius-server</td>
<td>39-10</td>
</tr>
<tr>
<td>aaa tacacs+-server</td>
<td>39-12</td>
</tr>
<tr>
<td>aaa tacacs command-authorization</td>
<td>39-15</td>
</tr>
<tr>
<td>aaa ldap-server</td>
<td>39-17</td>
</tr>
<tr>
<td>system fips admin-state</td>
<td>39-21</td>
</tr>
<tr>
<td>aaa authentication</td>
<td>39-23</td>
</tr>
<tr>
<td>aaa console admin-only</td>
<td>39-26</td>
</tr>
<tr>
<td>aaa authentication default</td>
<td>39-27</td>
</tr>
<tr>
<td>aaa accounting</td>
<td>39-29</td>
</tr>
<tr>
<td>aaa accounting command</td>
<td>39-31</td>
</tr>
<tr>
<td>aaa device-authentication</td>
<td>39-33</td>
</tr>
<tr>
<td>aaa accounting</td>
<td>39-35</td>
</tr>
<tr>
<td>aaa accounting radius calling-station-id</td>
<td>39-37</td>
</tr>
<tr>
<td>aaa 802.1x re-authentication</td>
<td>39-39</td>
</tr>
<tr>
<td>aaa interim-interval</td>
<td>39-41</td>
</tr>
<tr>
<td>aaa session-timeout</td>
<td>39-43</td>
</tr>
<tr>
<td>aaa session console</td>
<td>39-45</td>
</tr>
<tr>
<td>aaa inactivity-logout</td>
<td>39-47</td>
</tr>
<tr>
<td>aaa radius nas-port-id</td>
<td>39-49</td>
</tr>
<tr>
<td>aaa radius nas-identifier</td>
<td>39-50</td>
</tr>
<tr>
<td>aaa radius nas-ip-address</td>
<td>39-51</td>
</tr>
<tr>
<td>aaa radius mac-format</td>
<td>39-53</td>
</tr>
<tr>
<td>aaa profile</td>
<td>39-55</td>
</tr>
<tr>
<td>user</td>
<td>39-60</td>
</tr>
<tr>
<td>password</td>
<td>39-65</td>
</tr>
<tr>
<td>super-password</td>
<td>39-67</td>
</tr>
<tr>
<td>user password-size min</td>
<td>39-69</td>
</tr>
<tr>
<td>user password-expiration</td>
<td>39-71</td>
</tr>
<tr>
<td>user allow-ssh</td>
<td>39-73</td>
</tr>
<tr>
<td>user password-policy cannot-contain-username</td>
<td>39-75</td>
</tr>
<tr>
<td>user password-policy cannot-contain-consecutive-characters</td>
<td>39-77</td>
</tr>
<tr>
<td>user password-policy min-uppercase</td>
<td>39-79</td>
</tr>
<tr>
<td>user password-policy min-lowercase</td>
<td>39-80</td>
</tr>
<tr>
<td>user password-policy min-digit</td>
<td>39-81</td>
</tr>
<tr>
<td>user password-policy min-nonalpha</td>
<td>39-82</td>
</tr>
<tr>
<td>user password-history</td>
<td>39-84</td>
</tr>
<tr>
<td>user password-min-history</td>
<td>39-86</td>
</tr>
<tr>
<td>user lockout-window</td>
<td>39-88</td>
</tr>
<tr>
<td>user lockout-window</td>
<td>39-88</td>
</tr>
<tr>
<td>user lockout-threshold</td>
<td>39-90</td>
</tr>
<tr>
<td>user lockout-duration</td>
<td>39-92</td>
</tr>
<tr>
<td>user lockout unlock</td>
<td>39-94</td>
</tr>
<tr>
<td>show aaa server</td>
<td>39-96</td>
</tr>
<tr>
<td>show aaa server statistics</td>
<td>39-100</td>
</tr>
<tr>
<td>aaa radius-server clear-statistics</td>
<td>39-104</td>
</tr>
<tr>
<td>show aaa authentication</td>
<td>39-106</td>
</tr>
<tr>
<td>show aaa device-authentication</td>
<td>39-108</td>
</tr>
<tr>
<td>show aaa accounting</td>
<td>39-110</td>
</tr>
<tr>
<td>show aaa config</td>
<td>39-112</td>
</tr>
<tr>
<td>show aaa radius config</td>
<td>39-115</td>
</tr>
<tr>
<td>show aaa radius health-check-config</td>
<td>39-117</td>
</tr>
</tbody>
</table>
Chapter 40  Access Guardian Commands

unp dynamic-vlan-configuration .......................... 40-7
Contents

unp dynamic-profile-configuration ................................................................. 40-9
unp delay-learning ......................................................................................... 40-11
unp auth-server-down .................................................................................... 40-13
unp auth-server-down port-bounce ................................................................. 40-15
unp auth-server-down-timeout ....................................................................... 40-17
unp policy validity-period ............................................................................. 40-19
unp policy validity-location .......................................................................... 40-22
unp domain description ................................................................................. 40-24
unp redirect pause-timer .............................................................................. 40-26
unp redirect proxy-server-port ..................................................................... 40-28
unp redirect server ....................................................................................... 40-30
unp redirect allowed-name .......................................................................... 40-32
unp force-l3-learning .................................................................................... 40-34
unp 802.1x-pass-through ............................................................................ 40-37
unp ipv6-drop ............................................................................................... 40-39
unp ap-mode .................................................................................................. 40-40
unp mac-mobility .......................................................................................... 40-42
unp user flush .............................................................................................. 40-44
unp 802.1x eapol-version ............................................................................ 40-46
unp multi-untag-sap ..................................................................................... 40-47
unp profile .................................................................................................... 40-49
unp profile qos-policy-list ............................................................................ 40-52
unp profile location-policy .......................................................................... 40-54
unp profile period-policy ............................................................................. 40-56
unp profile captive-portal-authentication .................................................... 40-58
unp profile captive-portal-profile ................................................................. 40-60
unp profile kerberos-authentication ............................................................. 40-62
unp profile authentication-flag ................................................................... 40-64
unp profile mobile-tag .................................................................................. 40-66
unp profile maximum-ingress-bandwidth ..................................................... 40-68
unp profile maximum-egress-bandwidth ...................................................... 40-70
unp profile maximum-ingress-depth ............................................................. 40-72
unp profile maximum-egress-depth ............................................................... 40-74
unp profile inactivity-interval ..................................................................... 40-76
unp profile mac-mobility .............................................................................. 40-78
unp profile saa-profile .................................................................................. 40-80
unp profile map vlan .................................................................................... 40-82
unp profile map service-type spb ................................................................. 40-84
unp profile map service-type vxlan ............................................................... 40-88
unp vxlan far-end-ip-list ................................................................................ 40-92
unp profile map service-type l2gre .............................................................. 40-94
unp l2gre far-end-ip-list ................................................................................ 40-98
unp profile map service-type static ............................................................... 40-100
unp system-default service-mod ................................................................. 40-103
unp system-default service-base ................................................................. 40-105
unp system-default multicastmode ............................................................... 40-107
unp system-default vlan-xlation ................................................................. 40-109
unp system-default multicastgroup .............................................................. 40-111
unp system-default far-end-ip-list ............................................................... 40-113
unp saa-profile ............................................................................................ 40-115
unp port-type ............................................................................................... 40-117
unp l2-profile .............................................................................................. 40-120
Contents

unp redirect port-bounce .................................................................40-122
unp 802.1x-authentication ..............................................................40-124
unp 802.1x-authentication pass-alternate ........................................40-126
unp 802.1x-authentication tx-period ...............................................40-128
unp 802.1x-authentication supp-timeout .........................................40-130
unp 802.1x-authentication max-req ...............................................40-132
unp 802.1x-authentication bypass-8021x .......................................40-134
unp 802.1x-authentication failure-policy ........................................40-136
unp mac-authentication ..............................................................40-138
unp mac-authentication pass-alternate .........................................40-140
unp mac-authentication allow-eap ...............................................40-142
unp classification .................................................................40-144
unp trust-tag .................................................................................40-146
unp default-profile ...............................................................40-148
unp domain ..............................................................................40-150
unp aaa-profile ........................................................................40-152
unp port port-template ..............................................................40-154
unp direction ............................................................................40-156
unp admin-state .....................................................................40-158
unp dynamic-service ..............................................................40-160
unp vlan ..................................................................................40-162
unp port profile .......................................................................40-164
unp port ap-mode .................................................................40-166
unp port-template .............................................................40-168
unp network-group ..............................................................40-174
unp router-auth user-group ........................................................40-176
unp router-auth cp-profile ........................................................40-178
unp router-auth user flush .........................................................40-180
show unp network-group .........................................................40-182
show unp router-auth user-group ...............................................40-184
show unp router-auth configuration ............................................40-186
show unp router-auth users .......................................................40-188
unp classification port ...............................................................40-191
unp classification domain ........................................................40-194
unp classification mac-address ................................................40-196
unp classification mac-oui ........................................................40-199
unp classification mac-range ...................................................40-201
unp classification ip-address .....................................................40-204
unp classification vlan-tag ........................................................40-207
unp classification lldp med-endpoint ........................................40-209
unp classification authentication-type ......................................40-212
unp classification-rule ............................................................40-215
unp classification-rule port .......................................................40-218
unp classification-rule domain ................................................40-220
unp classification-rule mac-address ........................................40-222
unp classification-rule mac-oui ................................................40-224
unp classification-rule mac-range .............................................40-226
unp classification-rule ip-address .............................................40-228
unp classification-rule vlan-tag ...............................................40-230
unp classification-rule lldp med-endpoint ................................40-232
unp classification-rule authentication-type ................................40-234
unp classification-rule device-type ..........................................40-236
Contents

omniSwitch AOS Release 8 CLI Reference Guide  April 2023 xli

unp user-role ................................................................. 40-238
unp user-role policy-list ................................................. 40-240
unp user-role profile ..................................................... 40-242
unp user-role authentication-type ................................. 40-244
unp user-role cp-status-post-login ............................... 40-246
unp restricted-role policy-list ........................................ 40-248

show unp saa-profile ....................................................... 40-348
show unp vxlan far-end-ip-list ....................................... 40-344
show unp profile map ..................................................... 40-339
show unp profile ............................................................ 40-335

show zeroconf server policy-instances ......................... 40-333
show zeroconf service rules ......................................... 40-331
show zeroconf client policies ........................................ 40-329
show zeroconf server policies ....................................... 40-327
show zeroconf edge-details ............................................ 40-325
show zeroconf services-cache ........................................ 40-323

show zeroconf .................................................................. 40-318

zeroconf refresh-database ............................................. 40-316
zeroconf edge-ip-list mode ............................................ 40-314
zeroconf service-id query-request ................................. 40-310
zeroconf service-list ....................................................... 40-308
zeroconf service-id query-request ................................. 40-310
zeroconf edge-ip-list ..................................................... 40-312
zeroconf edge-ip-list mode ............................................ 40-314
zeroconf refresh-database ............................................. 40-316
show zeroconf ................................................................. 40-318

show zeroconf services ................................................... 40-321
show zeroconf services-cache ........................................ 40-323
show zeroconf edge-details ............................................. 40-325
show zeroconf server policies ........................................ 40-327
show zeroconf client policies ........................................ 40-329
show zeroconf service rules ........................................... 40-331
show zeroconf server policy-instances ......................... 40-333

show unp profile ........................................................... 40-335
show unp profile map ...................................................... 40-339
show unp vxlan far-end-ip-list ....................................... 40-344
show unp l2gre far-end-ip-list ....................................... 40-346
show unp saa-profile ...................................................... 40-348
show unp global configuration ................................................................. 40-350
show unp domain ................................................................................. 40-355
show unp classification ........................................................................ 40-357
show unp classification-rule ................................................................. 40-360
show unp user-role .............................................................................. 40-363
show unp restricted-role ...................................................................... 40-365
show unp port ........................................................................................ 40-367
show unp port config ........................................................................... 40-370
show unp port bandwidth ...................................................................... 40-375
show unp port 802.1x statistics ............................................................. 40-378
show unp port configured-vlans ............................................................ 40-380
show unp port profile .......................................................................... 40-382
show unp port-template ........................................................................ 40-384
show unp user ...................................................................................... 40-389
show unp user status ........................................................................... 40-393
show unp user details .......................................................................... 40-396
show unp policy validity-period ............................................................. 40-401
show unp policy validity-location ......................................................... 40-403
device-profile admin-state ................................................................. 40-405
device-profile port linkagg ................................................................. 40-406
device-profile device-type ................................................................. 40-408
device-profile update-signature ............................................................ 40-410
device-profile update-signature from .................................................. 40-411
device-profile auto-unp-assignment ...................................................... 40-413
show device-profile config ................................................................. 40-415
show device-profile summary ............................................................. 40-417
show device-profile catalog ............................................................... 40-419
show device-profile signatures from ................................................... 40-421
show device-profile signatures ........................................................... 40-423

Chapter 41 Application Monitoring and Enforcement Commands .................. 41-1
app-mon admin-state ............................................................................ 41-3
app-mon port admin-state ................................................................. 41-5
app-mon auto-group create ............................................................... 41-7
app-mon app-group .......................................................................... 41-9
app-mon app-list ................................................................................ 41-12
app-mon apply .................................................................................... 41-14
app-mon l3-mode .............................................................................. 41-16
app-mon l4-mode .............................................................................. 41-18
app-mon l4port-exclude .................................................................... 41-20
app-mon flow-table flush ................................................................. 41-22
app-mon flow-table enforcement stats .............................................. 41-24
app-mon aging enforcement ............................................................. 41-26
app-mon logging-threshold ............................................................... 41-28
app-mon flow-sync enforcement interval ......................................... 41-30
app-mon force-flow-sync ................................................................. 41-32
app-mon separate-config-file ........................................................... 41-33
app-mon data .................................................................................... 41-34
app-mon enforcement-mode ............................................................ 41-37
show app-mon config ....................................................................... 41-39
show app-mon port ............................................................................ 41-42
show app-mon app-pool ................................................................. 41-44
Chapter 42 Application Fingerprinting Commands ........................................ 42-1
    app-fingerprint admin-state .............................................................. 42-2
    app-fingerprint port ......................................................................... 42-4
    app-fingerprint signature-file .......................................................... 42-6
    app-fingerprint reload-signature-file ................................................. 42-8
    app-fingerprint trap .......................................................................... 42-9
    show app-fingerprint configuration .................................................. 42-10
    show app-fingerprint port .................................................................. 42-12
    show app-fingerprint app-name ......................................................... 42-14
    show app-fingerprint app-group ....................................................... 42-16
    show app-fingerprint database .......................................................... 42-18
    show app-fingerprint statistics ......................................................... 42-21

Chapter 43 FIP Snooping Commands ......................................................... 43-1
    fcoe fip-snooping ........................................................................... 43-3
    fcoe address-mode .......................................................................... 43-5
    fcoe priority .................................................................................... 43-7
    fcoe priority-protection ................................................................. 43-9
    fcoe priority-protection action ....................................................... 43-11
    fcoe filtering-resource trap-threshold ............................................. 43-13
    fcoe house-keeping-time-period ..................................................... 43-14
    fcoe vlan ......................................................................................... 43-15
    fcoe fcf mac ................................................................................... 43-17
    fcoe fc-map ...................................................................................... 43-19
    fcoe discovery-advertisement .......................................................... 43-21
    fcoe role ......................................................................................... 43-23
    show fcoe ....................................................................................... 43-26
    show fcoe ports ............................................................................... 43-29
    show fcoe sessions ......................................................................... 43-31
    show fcoe enode .............................................................................. 43-36
    show fcoe fcf .................................................................................. 43-38
    show fcoe fc-map ............................................................................ 43-40
    show fcoe discovery-advertisement ................................................. 43-42
    show fcoe statistics ........................................................................ 43-44
    clear fcoe statistics ........................................................................ 43-48

Chapter 44 FCoE/FC Gateway Commands ............................................. 44-1
    fibre-channel vsan .......................................................................... 44-4
    fibre-channel port mode .................................................................. 44-6
    fibre-channel vsan members ............................................................ 44-8
    fcoe vsan-map ................................................................................. 44-10
Port Mapping Commands

- port-mapping user-port network-port
- port-mapping unidirectional bidirectional
- port-mapping unknown-unicast-flooding
- port-mapping dynamic-proxy-arp
- show port-mapping status
- show port-mapping

Chapter 46

Port Mapping Commands

- port-mapping user-port network-port
- port-mapping unidirectional bidirectional
- port-mapping unknown-unicast-flooding
- port-mapping dynamic-proxy-arp
- show port-mapping status
- show port-mapping

Chapter 45

VXLAN Snooping Commands

- vm-snooping admin-state
- vm-snooping policy-mode
- vm-snooping trap
- vm-snooping filtering-resource trap threshold
- vm-snooping sampling-rate
- vm-snooping aging-timer
- vm-snooping vxlan udp-port
- vm-snooping static-policy rule
- vm-snooping logging-threshold
- vm-snooping port
- show vm-snooping config
- show vm-snooping port
- show vm-snooping database
- clear vm-snooping database
- show vm-snooping virtual-machines
- show vm-snooping filtering-resource
- show vm-snooping statistics
- show vm-snooping static-policy
- clear vm-snooping statistics
Chapter 47  Learned Port Security Commands .......................................................... 47-1
  port-security ......................................................................................................... 47-2
  port-security learning-window ............................................................................. 47-5
  port-security convert-to-static ............................................................................. 47-9
  port-security mac ................................................................................................. 47-11
  port-security maximum ........................................................................................ 47-14
  port-security learn-trap-threshold ....................................................................... 47-16
  port-security port max-filtering .......................................................................... 47-18
  port-security mac-range ....................................................................................... 47-20
  port-security port violation ................................................................................. 47-23
  port-security port pkt-relay ............................................................................... 47-25
  port-security pkt-relay protocol ........................................................................ 47-27
  port-security pkt-relay protocol udp ................................................................. 47-29
  show port-security pkt-relay filter ................................................................. 47-31
  show port-security ......................................................................................... 47-33
  show port-security mac-range ............................................................................ 47-36
  show port-security brief .................................................................................... 47-38
  show port-security learning-window .................................................................. 47-40

Chapter 48  Port Mirroring and Monitoring Commands ........................................... 48-1
  port-mirroring source destination ................................................................. 48-2
  port-mirroring .................................................................................................. 48-6
  port-mirroring traffic-priority .......................................................................... 48-8
  port-monitoring source .................................................................................... 48-9
  port-monitoring ............................................................................................... 48-12
  show port-mirroring status .............................................................................. 48-14
  show port-monitoring status ............................................................................ 48-16
  show port-monitoring file ............................................................................... 48-18

Chapter 49  sFlow Commands ................................................................................. 49-1
  sflow agent ..................................................................................................... 49-3
  sflow receiver ................................................................................................. 49-5
  sflow sampler .................................................................................................. 49-7
  sflow poller ..................................................................................................... 49-9
  show sflow agent ........................................................................................... 49-11
  show sflow receiver ....................................................................................... 49-13
  show sflow sampler ........................................................................................ 49-15
  show sflow poller ........................................................................................... 49-17

Chapter 50  RMON Commands .............................................................................. 50-1
  rmon probes ................................................................................................... 50-2
  show rmon probes ......................................................................................... 50-4
  show rmon events .......................................................................................... 50-7

Chapter 51  Switch Logging Commands ................................................................. 51-1
  swlog ............................................................................................................. 51-2
  swlog syslog-facility-id ............................................................................... 51-4
  swlog appid ................................................................................................... 51-6
  swlog output .................................................................................................. 51-9
  swlog output flash-file-size ............................................................................ 51-13
Chapter 52 Health Monitoring Commands

- health threshold ......................................................... 52-2
- health interval ......................................................... 52-5
- show health configuration ........................................ 52-7
- show health ................................................................. 52-9
- show health all ......................................................... 52-9

Chapter 53 Ethernet OAM Commands

- ethoam vlan ........................................................... 53-3
- ethoam domain ......................................................... 53-5
- ethoam domain mhf .................................................. 53-7
- ethoam domain id-permission .................................. 53-9
- ethoam association .................................................. 53-11
- ethoam association primary vlan ......................... 53-13
- ethoam association mhf ........................................... 53-15
- ethoam association id-permission ......................... 53-17
- ethoam association ccm-interval ......................... 53-19
- ethoam association endpoint-list ......................... 53-21
- ethoam association allowed-cvlan-list .................. 53-23
- clear ethoam statistics .......................................... 53-25
- ethoam default-domain level ......................... 53-27
- ethoam default-domain mhf .................................. 53-28
- ethoam default-domain id-permission ................ 53-29
- ethoam default-domain primary-vlan .................. 53-30
- ethoam endpoint ......................................................... 53-32
- ethoam endpoint admin-state ............................. 53-34
- ethoam endpoint rfp ................................................. 53-36
- ethoam endpoint ccm ............................................. 53-38
- ethoam endpoint priority ....................................... 53-40
- ethoam endpoint lowest-priority-defect ............. 53-42
- ethoam endpoint ctag-priority ............................ 53-44
- ethoam linktrace ......................................................... 53-46
- ethoam loopback ......................................................... 53-48
- ethoam fault-alarm-time ........................................ 53-50
- ethoam fault-reset-time ........................................ 53-52
- ethoam one-way-delay ........................................... 53-54
- ethoam two-way-delay ........................................... 53-56
- clear ethoam ............................................................. 53-58
- show ethoam ............................................................. 53-59
- show ethoam domain .............................................. 53-61
- show ethoam domain association ..................... 53-63
- show ethoam domain association end-point .......... 53-65
- show ethoam default-domain configuration .......... 53-69
Chapter 54 LINK OAM Commands ................................................................. 54-1
efm-oam admin-state ............................................................................ 54-3
efm-oam port admin-state ............................................................ 54-5
efm-oam port mode ............................................................................. 54-7
efm-oam port keepalive-interval .................................................... 54-9
efm-oam port hello-interval ............................................................. 54-11
efm-oam port remote-loopback ....................................................... 54-13
efm-oam port remote-loopback start ............................................ 54-15
efm-oam port propagate-events ....................................................... 54-17
efm-oam errored-frame-period ...................................................... 54-19
efm-oam errored-frame ............................................................... 54-21
efm-oam errored-frame-seconds-summary .................................... 54-23
efm-oam multiple-pdu-count .......................................................... 54-25
efm-oam port 11-ping ...................................................................... 54-26
show efm-oam configuration ........................................................... 54-28
show efm-oam port ........................................................................... 54-30
show efm-oam port detail ............................................................... 54-34
show efm-oam port statistics ............................................................ 54-37
show efm-oam port remote detail ................................................... 54-41
show efm-oam port history .............................................................. 54-43
show efm-oam port 11-ping detail .................................................. 54-45
clear efm-oam statistics ................................................................. 54-47
clear efm-oam log-history .............................................................. 54-49

Chapter 55 CPE Test Head Commands .................................................. 1-1
test-oam .......................................................... 1-3
test-oam direction ............................................................ 1-5
test-oam src-endpoint dst-endpoint ........................................... 1-7
test-oam port ............................................................................... 1-9
test-oam vlan test-frame ............................................................... 1-11
test-oam role .............................................................................. 1-13
test-oam duration rate packet-size ............................................. 1-15
test-oam frame ......................................................................... 1-17
test-oam l2-saa ........................................................................... 1-19
test-oam start stop .................................................................... 1-21
test-oam remote-sys-mac ............................................................ 1-23
test-oam statistics flash-logging ............................................... 1-25
show test-oam ........................................................................... 1-27
show test-oam statistics ............................................................ 1-31
show test-oam saa statistics ...................................................... 1-33
clear test-oam statistics ............................................................ 1-35
## Chapter 56 PPPoE Intermediate Agent

- `pppoe-ia` .............................................................................................................. 1-2
- `pppoe-ia {port | linkagg}` .................................................................................... 1-4
- `pppoe-ia {trust | client}` ...................................................................................... 1-6
- `pppoe-ia access-node-id` ..................................................................................... 1-8
- `pppoe-ia circuit-id` .............................................................................................. 1-10
- `pppoe-ia remote-id` ............................................................................................ 1-13
- `clear pppoe-ia statistics` .................................................................................... 1-15
- `show pppoe-ia configuration` ............................................................................. 1-17
- `show pppoe-ia {port | linkagg}` ........................................................................... 1-20
- `show pppoe-ia statistics` .................................................................................... 1-23

## Chapter 57 Service Assurance Agent Commands

- `saa` ......................................................................................................................... 2-2
- `saa type ip-ping` ............................................................................................... 2-4
- `saa type mac-ping` ............................................................................................. 2-6
- `saa spb` ................................................................................................................ 2-9
- `saa spb reset` ...................................................................................................... 2-12
- `saa spb flush` ...................................................................................................... 2-14
- `saa type ethoam-loopback` ................................................................................ 2-15
- `saa type ethoam-two-way-delay` ...................................................................... 2-18
- `saa start` ............................................................................................................. 2-21
- `saa stop` ............................................................................................................... 2-23
- `saa jitter-calculation enhanced` ........................................................................ 2-25
- `saa xml` ................................................................................................................. 2-27
- `show saa` ............................................................................................................. 2-29
- `show saa type config` ....................................................................................... 2-31
- `show saa spb` .................................................................................................... 2-36
- `show saa xml` ..................................................................................................... 2-38
- `show saa statistics` ............................................................................................ 2-40
- `show saa vrf` ...................................................................................................... 2-43

## Chapter 58 CMM Commands

- `reload secondary` .............................................................................................. 3-1
- `reload all` .......................................................................................................... 3-2
- `reload from` ...................................................................................................... 3-4
- `reload slot` ........................................................................................................ 3-6
## Chapter 59 Chassis Management and Monitoring Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>reload chassis-id</td>
<td>3-9</td>
</tr>
<tr>
<td>copy certified</td>
<td>3-11</td>
</tr>
<tr>
<td>issu from</td>
<td>3-13</td>
</tr>
<tr>
<td>issu slot</td>
<td>3-15</td>
</tr>
<tr>
<td>write memory</td>
<td>3-16</td>
</tr>
<tr>
<td>copy running certified</td>
<td>3-18</td>
</tr>
<tr>
<td>modify running-directory</td>
<td>3-20</td>
</tr>
<tr>
<td>copy flash-synchro</td>
<td>3-21</td>
</tr>
<tr>
<td>takeover</td>
<td>3-22</td>
</tr>
<tr>
<td>show running-directory</td>
<td>3-23</td>
</tr>
<tr>
<td>show reload</td>
<td>3-25</td>
</tr>
<tr>
<td>show microcode</td>
<td>3-27</td>
</tr>
<tr>
<td>usb</td>
<td>3-29</td>
</tr>
<tr>
<td>usb backup admin-state</td>
<td>3-31</td>
</tr>
<tr>
<td>usb auto-copy</td>
<td>3-34</td>
</tr>
<tr>
<td>mount</td>
<td>3-36</td>
</tr>
<tr>
<td>umount</td>
<td>3-37</td>
</tr>
<tr>
<td>show usb statistics</td>
<td>3-38</td>
</tr>
<tr>
<td>show issu status</td>
<td>3-40</td>
</tr>
<tr>
<td>auto-config-abort</td>
<td>3-42</td>
</tr>
<tr>
<td>image integrity check</td>
<td>3-43</td>
</tr>
<tr>
<td>image integrity get-key</td>
<td>3-45</td>
</tr>
</tbody>
</table>
Chapter 60  Network Time Protocol Commands  

ntp server .................................................................................................................. 5-1  
ntp server synchronized .......................................................................................... 5-3  
ntp server unsynchronized ...................................................................................... 5-7  
ntp client .................................................................................................................... 5-8  
ntp src-ip preferred .................................................................................................. 5-9  
ntp broadcast-client ................................................................................................. 5-11  
ntp broadcast-delay ................................................................................................. 5-13  
ntp broadcast-client ................................................................................................. 5-15
Chapter 62  
**File Management Commands**  
- show ssh .......................................................................................... 6-55  
- cd ........................................................................................................... 7-2  
- pwd ......................................................................................................... 7-4  
- mkdir ..................................................................................................... 7-6  
- rmdir ..................................................................................................... 7-8  
- ls ............................................................................................................ 7-10  
- rm .......................................................................................................... 7-12  
- cp .......................................................................................................... 7-14  
- scp ........................................................................................................ 7-16  
- mv .......................................................................................................... 7-18  
- chmod .................................................................................................... 7-20  
- freespace ............................................................................................. 7-21  
- fsck ....................................................................................................... 7-23  
- newfs .................................................................................................... 7-25  
- vi ......................................................................................................... 7-27  
- tty ......................................................................................................... 7-29  
- show tty ............................................................................................... 7-31  
- tftp ....................................................................................................... 7-32  
- sftp ....................................................................................................... 7-34  
- ftp ......................................................................................................... 7-36  
- show ftp ............................................................................................... 7-38  

Chapter 63  
**Web Management Commands**  
- webview server ................................................................................... 8-2  
- webview access .................................................................................... 8-4  
- webview force-ssl ............................................................................... 8-6  
- webview http-port ............................................................................. 8-8  
- webview https-port ........................................................................... 8-10  
- webview ssl-strong-ciphers .............................................................. 8-12  
- webview wlan cluster-virtual-ip precedence .................................... 8-14  
- webview wlan cluster-virtual-ip .......................................................... 8-16  
- show webview wlan config ................................................................. 8-17  
- show webview .................................................................................... 8-19  

Chapter 64  
**Configuration File Manager Commands**  
- configuration apply ......................................................................... 9-2  
- configuration error-file-limit ............................................................... 9-4  
- show configuration status ................................................................. 9-6  
- configuration cancel ........................................................................ 9-8  
- configuration syntax-check ............................................................... 9-9  
- configuration snapshot .................................................................... 9-11  
- show configuration snapshot ............................................................ 9-13  
- write terminal .................................................................................. 9-15  
- configuration backup restore ......................................................... 9-16  
- configuration apply network-sync .................................................. 9-18  

Chapter 65  
**SNMP Commands**  
- snmp station .................................................................................... 10-3  
- show snmp station .......................................................................... 10-6  
- snmp snmp-engineid-type .............................................................. 10-8
Contents

show snmp snmp-engineid ................................................................. 10-10
snmp community-map ........................................................................ 10-12
snmp community-map mode .............................................................. 10-14
show snmp community-map .............................................................. 10-16
snmp security .................................................................................... 10-18
snmp security tsm ............................................................................. 10-20
snmp tsm-map .................................................................................... 10-21
show snmp tsm-map ............................................................................ 10-23
show snmp security ............................................................................. 10-25
show snmp statistics ........................................................................... 10-27
show snmp mib-family ........................................................................ 10-29
snmp-trap absorption ........................................................................ 10-31
snmp-trap to-webview ........................................................................ 10-33
snmp-trap replay-ip ............................................................................ 10-34
snmp-trap filter-ip .............................................................................. 10-36
snmp authentication-trap ................................................................. 10-38
show snmp-trap replay-ip ................................................................... 10-39
show snmp-trap filter-ip ...................................................................... 10-41
show snmp authentication-trap ......................................................... 10-43
show snmp-trap config ....................................................................... 10-44
event-action ....................................................................................... 10-46
show event-action .............................................................................. 10-48

Chapter 66  OmniVista Cirrus Commands ...................................................... 64-1
cloud-agent admin-state ................................................................. 64-2
cloud-agent discovery-interval ......................................................... 64-4
cloud-agent remove-inconsistent-certificate ..................................... 64-6
show cloud-agent status ................................................................... 64-8
show cloud-agent vpn status ............................................................ 64-10
naas license call-home interval .......................................................... 64-12
naas license apply file ....................................................................... 64-14
show naas license .............................................................................. 64-15
show naas-agent status ...................................................................... 64-17

Chapter 67  OpenFlow Commands ............................................................... 65-1
openflow back-off-max ....................................................................... 65-2
openflow idle-probe-timeout ............................................................... 65-3
openflow logical-switch ...................................................................... 65-4
openflow logical-switch controller ...................................................... 65-7
openflow logical-switch interfaces ...................................................... 65-9
show openflow .................................................................................. 65-11
show openflow logical-switch ............................................................ 65-13

Chapter 68  DNS Commands ............................................................... 66-1
ip domain-lookup .............................................................................. 66-2
ip name-server .................................................................................. 66-4
ipv6 name-server .............................................................................. 66-6
ip domain-name ................................................................................ 66-8
show dns ......................................................................................... 66-10

Appendix A  Software License and Copyright Statements ................................ A-1
Contents

ALE USA, Inc. License Agreement ................................................................. A-1
ALE USA, INC. SOFTWARE LICENSE AGREEMENT ................................. A-1
Third Party Licenses and Notices .............................................................. A-4

CLI Quick Reference

Index ........................................................................................................... Index-1
About This Guide

This *OmniSwitch AOS Release 8 CLI Reference Guide* is a comprehensive resource to all Command Line Interface (CLI) commands available on the OmniSwitch.

Supported Platforms

The information in this guide applies only to the following products:

- OmniSwitch 6360 Series
- OmniSwitch 6465 Series
- OmniSwitch 6560 Series
- OmniSwitch 6570M Series
- OmniSwitch 6860 Series
- OmniSwitch 6865 Series
- OmniSwitch 6900 Series
- OmniSwitch 9900 Series

Who Should Read this Manual?

The audience for this user guide is network administrators and IT support personnel who need to configure, maintain, and monitor switches and routers in a live network. Anyone wishing to gain knowledge on the details of all CLI commands available on the OmniSwitch will benefit from the material in this reference guide. However, advanced users who have already familiarized themselves with the OmniSwitch CLI commands will benefit most from the detailed content in this guide.

When Should I Read this Manual?

Read this guide whenever you want detailed information on individual CLI commands. Although this guide provides helpful information during any stage of the configuration process, it is a good idea to first familiarize yourself with the software features available on the switch before investigating the detailed command information in this guide.

Overview information, procedures, and live network examples on switch software features can be found in the *OmniSwitch AOS Release 8 Switch Management Guide*, *OmniSwitch AOS Release 8 Network Configuration Guide*, *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide*, and *OmniSwitch AOS Release 8 Data Center Switching Guide*. Once you are familiar with the procedures and
base CLI commands in these configuration guides you can obtain more detailed information on the individual commands in this guide.
What is in this Manual?

This reference guide includes information on every CLI command available in the switch. Command reference information is included for base software commands as well as commands associated with optional software packages, such as Advanced Routing (multicast routing protocols and OSPF). The information provided for each CLI command includes:

- Command description.
- Syntax.
- Description of all keywords and variables included in the syntax.
- Default values.
- Usage guidelines, which include tips on when and how to use the command.
- Examples of command lines using the command.
- Related commands with descriptions.
- Release history, which indicates the release when the command was introduced.
- SNMP information, such as the MIB files related to a set of CLI commands. In addition each CLI command includes the corresponding MIB variables that map to all parameters included in a command.

What is Not in this Manual?

Primarily a reference, this guide does not provide step-by-step instructions on how to set up particular features on the switch. It also does not provide overview or application examples on software features. For comprehensive information on how to configure particular software features in the switch, consult the appropriate configuration guide.

This guide also does not provide any information on the network management applications, WebView and OmniVista. Further information on WebView and OmniVista can be found in the context-sensitive on-line help available with those applications.

How is the Information Organized?

Each chapter in this guide includes reference material for all commands related to a single software feature, such as server load balancing or link aggregation. Typically commands in a single chapter will share a common prefix.
## Text Conventions

The following table contains text conventions and usage guidelines for CLI commands as they are documented in this guide.

<table>
<thead>
<tr>
<th>Text Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold text</strong></td>
<td>Indicates basic command and keyword syntax.</td>
</tr>
<tr>
<td>Example:</td>
<td><em>show snmp station</em></td>
</tr>
<tr>
<td><strong>italicized text</strong></td>
<td>Indicates user-specific information such as IP addresses, slot numbers, passwords, names, etc.</td>
</tr>
<tr>
<td>Example:</td>
<td><em>no snmp station ip_address</em></td>
</tr>
<tr>
<td></td>
<td>Italicized text that is not enclosed with straight brackets ([ ]) indicates required information.</td>
</tr>
<tr>
<td><strong>[]</strong> (Straight Brackets)</td>
<td>Indicates optional parameters for a given command.</td>
</tr>
<tr>
<td>Example:</td>
<td><em>show aaa server [server_name]</em></td>
</tr>
<tr>
<td></td>
<td>Here, you can enter either of the following options:</td>
</tr>
<tr>
<td></td>
<td><em>show aaa server</em></td>
</tr>
<tr>
<td></td>
<td><em>show aaa server server_name</em> (where server_name is the user-specified server name, e.g., show aaa server myserver1)</td>
</tr>
<tr>
<td></td>
<td>Note that this example includes <em>italicized text</em>. The optional parameter in this case is a user-specified server name.</td>
</tr>
<tr>
<td><strong>{}</strong> (Curly Braces)</td>
<td>Indicates that the user must choose between one or more parameters.</td>
</tr>
<tr>
<td>Example:</td>
<td>*port mirroring {enable</td>
</tr>
<tr>
<td></td>
<td>Here, you must choose one of the following:</td>
</tr>
<tr>
<td></td>
<td><em>port mirroring enable</em></td>
</tr>
<tr>
<td></td>
<td><em>port mirroring disable</em></td>
</tr>
<tr>
<td>**</td>
<td>** (Vertical Pipes)</td>
</tr>
<tr>
<td>Example:</td>
<td>*show health threshold [rx</td>
</tr>
<tr>
<td></td>
<td>separates the choices <em>rx, txrx, memory</em>, and <em>cpu</em>.</td>
</tr>
<tr>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td><em>show health threshold rx</em></td>
</tr>
<tr>
<td></td>
<td><em>show health threshold txrx</em></td>
</tr>
<tr>
<td></td>
<td><em>show health threshold memory</em></td>
</tr>
<tr>
<td></td>
<td><em>show health threshold cpu</em></td>
</tr>
<tr>
<td><strong>&quot; &quot;</strong> (Quotation Marks)</td>
<td>Used to enclose text strings that contain spaces. The quotation marks are required input on the command line.</td>
</tr>
<tr>
<td>Example:</td>
<td><em>vlan 2 &quot;new test vlan&quot;</em></td>
</tr>
</tbody>
</table>
Documentation Roadmap

The OmniSwitch user documentation suite was designed to supply you with information at several critical junctures of the configuration process. The following section outlines a roadmap of the manuals that will help you at each stage of the configuration process. Under each stage, we point you to the manual or manuals that will be most helpful to you.

**Stage 1: Using the Switch for the First Time**

**Pertinent Documentation:** *OmniSwitch Hardware Users Guide*  
*Release Notes*

This guide provides all the information you need to get your switch up and running the first time. It provides information on unpacking the switch, rack mounting the switch, installing NI modules, unlocking access control, setting the switch’s IP address, and setting up a password. It also includes succinct overview information on fundamental aspects of the switch, such as hardware LEDs, the software directory structure, CLI conventions, and web-based management.

At this time you should also familiarize yourself with the Release Notes that accompanied your switch. This document includes important information on feature limitations that are not included in other user guides.

**Stage 2: Gaining Familiarity with Basic Switch Functions**

**Pertinent Documentation:** *OmniSwitch Hardware Users Guide*  
*OmniSwitch AOS Release 8 Switch Management Guide*

Once you have your switch up and running, you will want to begin investigating basic aspects of its hardware and software. Information about switch hardware is provided in the *OmniSwitch Hardware Users Guide*. This guide provide specifications, illustrations, and descriptions of all hardware components, such as chassis, power supplies, Chassis Management Modules (CMMs), Network Interface (NI) modules, and cooling fans. It also includes steps for common procedures, such as removing and installing switch components.

The *OmniSwitch AOS Release 8 Switch Management Guide* is the primary users guide for the basic software features on a single switch. This guide contains information on the switch directory structure, basic file and directory utilities, switch access security, SNMP, and web-based management. It is recommended that you read this guide before connecting your switch to the network.

**Stage 3: Integrating the Switch Into a Network**

**Pertinent Documentation:** *OmniSwitch AOS Release 8 Network Configuration Guide*  
*OmniSwitch AOS Release 8 Advanced Routing Configuration Guide*  
*OmniSwitch AOS Release 8 Data Center Switching Guide*

When you are ready to connect your switch to the network, you will need to learn how the OmniSwitch implements fundamental software features, such as 802.1Q, VLANs, Spanning Tree, and network routing protocols. The *OmniSwitch AOS Release 8 Network Configuration Guide* contains overview information, procedures, and examples on how standard networking technologies are configured on the OmniSwitch.

The *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide* includes configuration information for networks using advanced routing technologies (OSPF and BGP) and multicast routing protocols (DVMRP and PIM-SM).
The *OmniSwitch AOS Release 8 Data Center Switching Guide* includes configuration information for data center networks using virtualization technologies, such as Data Center Bridging (DCB) protocols, Virtual eXtensible LAN (VxLAN), and Fibre Channel over Ethernet (FCoE) network convergence.

**Anytime**

The *OmniSwitch AOS Release 8 CLI Reference Guide* contains comprehensive information on all CLI commands supported by the switch. This guide includes syntax, default, usage, example, related CLI command, and CLI-to-MIB variable mapping information for all CLI commands supported by the switch. This guide can be consulted anytime during the configuration process to find detailed and specific information on each CLI command.
Related Documentation

The following are the titles and descriptions of all the related OmniSwitch user manuals:

- **OmniSwitch 6360, 6465, 6560, 6570M, 6860, 6865, 6900, 9900 Hardware Users Guides**
  Describes the hardware and software procedures for getting an OmniSwitch up and running as well as complete technical specifications and procedures for all OmniSwitch chassis, power supplies, fans, and Network Interface (NI) modules.

- **OmniSwitch AOS Release 8 CLI Reference Guide**
  Complete reference to all CLI commands supported on the OmniSwitch. Includes syntax definitions, default values, examples, usage guidelines and CLI-to-MIB variable mappings.

- **OmniSwitch AOS Release 8 Switch Management Guide**
  Includes procedures for readying an individual switch for integration into a network. Topics include the software directory architecture, image rollback protections, authenticated switch access, managing switch files, system configuration, using SNMP, and using web management software (WebView).

- **OmniSwitch AOS Release 8 Network Configuration Guide**
  Includes network configuration procedures and descriptive information on all the major software features and protocols included in the base software package. Chapters cover Layer 2 information (Ethernet and VLAN configuration), Layer 3 information (routing protocols, such as RIP and IPX), security options (authenticated VLANs), Quality of Service (QoS), link aggregation, and server load balancing.

- **OmniSwitch AOS Release 8 Advanced Routing Configuration Guide**
  Includes network configuration procedures and descriptive information on all the software features and protocols included in the advanced routing software package. Chapters cover multicast routing (DVMRP and PIM-SM), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP).

- **OmniSwitch AOS Release 8 Data Center Switching Guide**
  Includes an introduction to the OmniSwitch data center switching architecture as well as network configuration procedures and descriptive information on all the software features and protocols that support this architecture. Chapters cover Data Center Bridging (DCB) protocols, Virtual Network Profile (vNP), VxLAN, and FCoE/FC transit and gateway functionality.

- **OmniSwitch AOS Release 8 Transceivers Guide**
  Includes SFP and XFP transceiver specifications and product compatibility information.

- **OmniSwitch AOS Release 8 Specifications Guide**

- **Technical Tips, Field Notices**
  Includes information published by Alcatel-Lucent Enterprise’s Customer Support group.

- **Release Notes**
  Includes critical Open Problem Reports, feature exceptions, and other important information on the features supported in the current release and any limitations to their support.
Technical Support

An Alcatel-Lucent Enterprise service agreement brings your company the assurance of 7x24 no-excuses technical support. You’ll also receive regular software updates to maintain and maximize your Alcatel-Lucent Enterprise product’s features and functionality and on-site hardware replacement through our global network of highly qualified service delivery partners.

With 24-hour access to Alcatel-Lucent Enterprise’s Service and Support web page, you’ll be able to view and update any case (open or closed) that you have reported to Alcatel-Lucent Enterprise’s technical support, open a new case or access helpful release notes, technical bulletins, and manuals.

Access additional information on Alcatel-Lucent Enterprise’s Service Programs:

   Web: https://myportal.al-enterprise.com
   Phone: 1-800-995-2696
   Email: ebg_global_supportcenter@al-enterprise.com
1 Ethernet Port Commands

The Ethernet port software is responsible for configuring and monitoring Ethernet ports. This includes:

• Performing hardware diagnostics, loading software, and initializing hardware.

• Notifying other software modules in the system when Ethernet links become active or inactive.

• Configuring basic line parameters for Ethernet ports.

• Gathering basic line statistics for Ethernet ports and passing this information to the user interface and configuration manager.

MIB information for the Ethernet Port commands is as follows:

 Filename: ALCATEL-IND1-PORT-MIB.mib
 Module: alcatelIND1PortMIB

 Filename: EtherLike-MIB.mib
 Module: etherMIB
A summary of the available commands is listed here.

<table>
<thead>
<tr>
<th>Interfaces commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>interfaces</td>
<td></td>
</tr>
<tr>
<td>interfaces speed</td>
<td></td>
</tr>
<tr>
<td>interfaces crossover</td>
<td></td>
</tr>
<tr>
<td>interfaces duplex</td>
<td></td>
</tr>
<tr>
<td>interfaces alias</td>
<td></td>
</tr>
<tr>
<td>clear interfaces</td>
<td></td>
</tr>
<tr>
<td>interfaces max-frame-size</td>
<td></td>
</tr>
<tr>
<td>interfaces inter-frame-gap</td>
<td></td>
</tr>
<tr>
<td>interfaces flood-limit</td>
<td></td>
</tr>
<tr>
<td>interfaces flood-limit action</td>
<td></td>
</tr>
<tr>
<td>interfaces ingress-bandwidth</td>
<td></td>
</tr>
<tr>
<td>interfaces pause</td>
<td></td>
</tr>
<tr>
<td>interfaces link-trap</td>
<td></td>
</tr>
<tr>
<td>interfaces ddm</td>
<td></td>
</tr>
<tr>
<td>interfaces ddm-trap</td>
<td></td>
</tr>
<tr>
<td>interfaces wait-to-restore</td>
<td></td>
</tr>
<tr>
<td>interfaces wait-to-shutdown</td>
<td></td>
</tr>
<tr>
<td>interfaces eee</td>
<td></td>
</tr>
<tr>
<td>interfaces primary-port split-mode</td>
<td></td>
</tr>
<tr>
<td>interfaces port break-out</td>
<td></td>
</tr>
<tr>
<td>interfaces hybrid-mode</td>
<td></td>
</tr>
<tr>
<td>interfaces loopback</td>
<td></td>
</tr>
<tr>
<td>interfaces portgroup</td>
<td></td>
</tr>
<tr>
<td>clear violation</td>
<td></td>
</tr>
<tr>
<td>show interfaces</td>
<td></td>
</tr>
<tr>
<td>show interfaces alias</td>
<td></td>
</tr>
<tr>
<td>show interfaces status</td>
<td></td>
</tr>
<tr>
<td>show interfaces capability</td>
<td></td>
</tr>
<tr>
<td>show interfaces accounting</td>
<td></td>
</tr>
<tr>
<td>show interfaces counters</td>
<td></td>
</tr>
<tr>
<td>show interfaces counters errors</td>
<td></td>
</tr>
<tr>
<td>show interfaces flood-rate</td>
<td></td>
</tr>
<tr>
<td>show interfaces traffic</td>
<td></td>
</tr>
<tr>
<td>show interfaces ingress-rate-limit</td>
<td></td>
</tr>
<tr>
<td>show interfaces ddm</td>
<td></td>
</tr>
<tr>
<td>show interfaces split-mode</td>
<td></td>
</tr>
<tr>
<td>show interfaces break-out</td>
<td></td>
</tr>
<tr>
<td>show violation</td>
<td></td>
</tr>
<tr>
<td>show interfaces portgroup</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface violation commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>violation recovery-maximum</td>
<td></td>
</tr>
<tr>
<td>violation recovery-time</td>
<td></td>
</tr>
<tr>
<td>violation recovery-trap</td>
<td></td>
</tr>
<tr>
<td>show violation</td>
<td></td>
</tr>
<tr>
<td>show interfaces portgroup</td>
<td></td>
</tr>
<tr>
<td>clear violation</td>
<td></td>
</tr>
</tbody>
</table>
### Ethernet Port Commands

<table>
<thead>
<tr>
<th>Category</th>
<th>Commands</th>
</tr>
</thead>
</table>
| Link monitoring commands | interfaces link-monitoring admin-status  
| interfaces link-monitoring time-window  
| interfaces link-monitoring link-flap-threshold  
| interfaces link-monitoring link-error-threshold  
| interfaces clear-link-monitoring-stats  
| show interfaces link-monitoring config  
| show interfaces link-monitoring statistics |
| Time Domain Reflectometry (TDR) commands | interfaces tdr  
| show interfaces tdr-statistics |
| Link fault propagation commands | link-fault-propagation group  
| link-fault-propagation group source  
| link-fault-propagation group destination  
| link-fault-propagation group wait-to-shutdown  
| show link-fault-propagation group |
| LED beacon commands | interfaces beacon  
| show interfaces beacon |
| IEEE 1588 Precision Time Protocol (PTP) commands | interfaces ptp admin-state  
| interfaces port ptp p2p  
| show interfaces ptp config |
| MAC Security commands | interfaces macsec admin-state  
| interfaces macsec key-rotation max-session-time  
| interfaces macsec key-rotation max-exchange-data  
| show interfaces macsec  
| show interfaces macsec static  
| show interfaces macsec dynamic  
| show interfaces macsec statistics  
| show interfaces macsec dynamic key-rotation  
| clear interfaces macsec statistics |
**interfaces**

Enables or disables auto negotiation or administrative status on a single port, a range of ports, or an entire Network Interface (NI).

```
interfaces {slot chassis/slot| port chassis/slot/port[-port2]} {admin-state | autoneg | epp} {enable |

disable}
```

### Syntax Definitions

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.
- `admin-state enable` Enables administrative state.
- `admin-state disable` Disables administrative state.
- `autoneg enable` Enables auto negotiation.
- `autoneg disable` Disables auto negotiation.
- `epp enable` Enables Enhanced Port Performance.
- `epp disable` Disables Enhanced Port Performance.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If auto negotiation is disabled, auto MDIX, flow control, auto speed, and auto duplex are not accepted. See the **interfaces crossover** command on page 1-8 and the **interfaces duplex** command on page 1-10 for more information.

- When EPP is enabled the fiber port receiver performance is enhanced by increasing its sampling rate. This enhancement can help with port link connection reliability or CRC problems that may occur with direct copper cable interfaces.

- Autonegotiation cannot be disabled on 10GBase-T ports.
- The 2.5G capable ports will advertise either 2.5G or 1G when auto-negotiation is enabled depending on the port's configured speed. The default is 2.5G.

- Autonegotiation is disabled for 10G port types and optical transceivers. It is enabled for 25G, 40G, and 100G direct-attached cables.

- OS6860N models don't support auto-negotiation on SFP28 ports when a 1G transceiver is connected.

**Examples**

-> interfaces port 1/3/1 autoneg disable
-> interfaces slot 1/3 autoneg disable
-> interfaces port 1/3/1-4 autoneg disable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **interfaces speed**: Configures interface speed.
- **interfaces crossover**: Configures crossover port settings.
- **interfaces duplex**: Enables or disables flow (pause).
- **show interfaces alias**: Displays interface line settings.
- **show interfaces**: Displays auto negotiation, speed, duplex, and crossover settings.

**MIB Objects**

- **esmConfTable**: esmPortCfgAutoNegotiation
**interfaces speed**

Configures interface line speed.

```
interfaces {slot chassis/slot | port chassis/slot/port [-port2]} speed {10 | 100 | 1000 | 2500 | 10000 | 2000 | 4000 | 8000 | auto | max {100 | 1000 | 4000 | 8000}}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.
- **auto**: The switch automatically sets the line speed to match the attached device (auto-sensing).
- **10**: Sets the interface to 10 Mbps.
- **100**: Sets the interface to 100 Mbps.
- **1000**: Sets the interface to 1000 Mbps (1 Gigabit).
- **2500**: Sets the interface to 2500 Mbps (2.5 Gigabits).
- **4000**: Sets the interface to 4000 Mbps for FibreChannel.
- **8000**: Sets the interface to 8000 Mbps for FibreChannel.
- **max 100**: Sets the maximum speed to 100 Mbps.
- **max 1000**: Sets the maximum speed to 1000 Mbps (1 Gigabit).
- **max 4000**: Sets the maximum speed to 4000 Mbps for FibreChannel.
- **max 8000**: Sets the maximum speed to 8000 Mbps for FibreChannel.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>enable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- The changing of a port's speed, when changing between 100M/1G and 2.5G or vice-versa, is applied in port pairs. Meaning, changing the speed of one port of a pair will cause the other port's speed to change as well. The port pairs are 17/18, 19/20, 21/22, 23/24. This does not apply when changing the speed between 100M and 1G.

- Certain port groups don't support a mix of 1G/10G and 25G speeds on the ports within a group. Ports within a port group must all run at either 1G/10G speed or 25G speed. Mixing 1G and 10G speeds is supported. Refer to the respective hardware guide for additional information.
  - OS6900-V48C8 Port Groups (1,2,3,6), (4,5,7,9), (8,10,11,12), (13,14,15,18), (16,17,19,21), (20,22,23,24), (25,26,27,30), (28,29,31,33), (32,34,35,36), (37,38,39,42), (40,41,43,45), (44,46,47,48)
  - OS6900-X48C4E Port Groups (41,44, 45-48)
  - OS6860N-U28 Port Group (31-34)
  - OS6860N-P48Z Port Group (51-54)
  - OS6860N-P24Z Port Group (27-30)
  - OS68-VNI-U4 Port Group (1-4)

**Examples**

- `-> interfaces slot 1/3 speed auto`
- `-> interfaces port 1/3/1 speed 100`
- `-> interfaces port 1/3/2-8 speed 1000`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show interfaces` Displays auto negotiation, speed, duplex, and crossover settings.

**MIB Objects**

- `esmConfTable`
- `esmPortCfgSpeed`
**interfaces crossover**

Configures port crossover settings on a single port, a range of ports, or an entire Network Interface (NI).

```
interfaces {slot chassis/slot| port chassis/slot/port[-port2]} crossover {auto | mdix | mdi}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.
- **auto**: The interface automatically detects the crossover settings.
- **mdix**: Sets the crossover configuration to Media Dependent Interface with Crossover (MDIX), which is the standard for hubs and switches.
- **mdi**: Sets the crossover configuration to Media Dependent Interface (MDI), which is the standard for end stations.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>mdix</td>
</tr>
</tbody>
</table>

### Platforms Supported

Not supported in this release.

### Usage Guidelines

- If auto negotiation is disabled, then automatic crossover is also disabled. See the `interfaces` command for more information.
- You cannot configure crossover settings on fiber ports. These ports use the MDI standard.

### Examples

```
-> interfaces slot 1/3 crossover mdi
-> interfaces port 1/3/1 crossover mdix
-> interfaces port 1/3/1-4 crossover auto
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

*show interfaces*  
Displays auto negotiation, speed, duplex, and crossover settings.

**MIB Objects**

*esmConfTable*

  *esmPortCfgCrossover*
**interfaces duplex**

Configures duplex mode. In full duplex mode, the interface transmits and receives data simultaneously. In half duplex mode, the interface can transmit or receive data at a given time. Auto duplex setting causes the switch to advertise all available duplex modes (half/full/both) for the port during autonegotiation.

```
interfaces {slot chassis/slot| port chassis/slot/port)[-port2]} duplex {full | half | auto}
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.
- `full` Sets interface to full duplex mode.
- `half` Sets interface to half duplex mode.
- `auto` Switch automatically sets both the duplex mode settings to autonegotiation.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>full</td>
<td>half</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- You can only configure one slot at a time. Repeat the command to configure additional slots.
- The OmniSwitch 6860(E)/6865/6900 do not support 10/100 half-duplex.
- Half duplex mode is not supported on Gigabit modules if a port is detected as Gigabit (1000 Mbps).
- Gigabit and 10 Gigabit fiber ports only support full duplex.

**Examples**

- `-> interfaces port 1/3/1 duplex auto`
- `-> interfaces slot 1/3 duplex half`
- `-> interfaces port 1/3/1-4 auto`
**Release History**
Release 7.1.1; command introduced.

**Related Commands**

- **interfaces**
  Configures interface line speed. Set to `auto` to set speed and duplex mode to auto-sensing.

- **show interfaces**
  Displays auto negotiation, speed, duplex, and crossover settings.

**MIB Objects**

- **esmConfTable**
  - **esmPortAutoDuplexMode**
interfaces alias

Configures a description (alias) for a single port.

`interfaces port chassis/slot/port alias description`

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number.
- **description**: A description for the port, which can be up to 64 characters long. Description tags with spaces must be enclosed within quotes (e.g., “IP Phone”).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- You can only configure one port at time. You cannot configure an alias for multiple ports.
- To remove an alias use a description consisting of two quotes without any spaces (e.g., "").

### Examples

- `-> interfaces port 1/3/1 alias "switch port"
- `-> interfaces port 1/2/2 alias "IP Phone"
- `-> interfaces port 1/3/1 alias ""

### Release History

Release 7.1.1; command introduced.
Related Commands

**show interfaces alias**  Displays port status (up or down) and any aliases for a port.

MIB Objects

*ifXTable*

  *ifAlias*

---
clear interfaces

Resets all Layer 2 statistics counters or Time Domain Reflectometry (TDR) statistics counters.

clear interfaces {slot chassis/slot | port chassis/slot/port[-port2]} {l2-statistics [cli] | tdr-statistics}

**Syntax Definitions**

- **chassis**
  - The chassis identifier when running in virtual chassis mode.
- **slot**
  - The slot number for a specific module.
- **port[-port2]**
  - The port number. Use a hyphen to specify a range of ports.
- **cli**
  - Clears the CLI statistics only.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- TDR is supported only on the OmniSwitch 6860 and OmniSwitch 6860.
- There is no global clear statistics command for TDR. The highest level granularity supported for clearing statistics is per `chassis/slot`.

**Examples**

- `-> clear interfaces port 1/1/20 l2-statistics`
- `-> clear interfaces port 1/1/30 l2-statistics cli`
- `-> clear interfaces port 1/1/40 tdr-statistics`

**Release History**

Release 7.1.1; command introduced.
Release 8.1.1; `tdr-statistics` parameter added.
**Related Commands**

- **show interfaces counters** Displays general interface information, including when statistics were last cleared.
- **show interfaces tdr-statistics** Displays the results of the last TDR test performed on a port.

**MIB Objects**

- **alcetherStatsTable**
  - **alcetherClearStats**
- **esmTdrPortTable**
  - **esmTdrPortClearResults**
interfaces max-frame-size

Configures the maximum frame size for Gigabit Ethernet interfaces.

`interfaces {slot chassis/slot | port chassis/slot/port[-port2]} max-frame-size bytes`

**Syntax Definitions**

- `chassis`  The chassis identifier.
- `slot`     The slot number for a specific module.
- `port[-port2]`  The port number. Use a hyphen to specify a range of ports.
- `bytes`     Maximum frame size, in bytes. Valid range is 1518–9216.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes (Gigabit Ethernet Packets)</td>
<td>9216</td>
</tr>
<tr>
<td>bytes (Ethernet Packets)</td>
<td>1553</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `-> interfaces port 1/3/1 max-frame-size 1518`
- `-> interfaces slot 1/3 max-frame-size 1518`

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

`show interfaces`  
Displays auto negotiation, speed, duplex, and crossover settings.

**MIB Objects**

`esmConfTable`  
`esmPortCfgMaxFrameSize`
interfaces inter-frame-gap

Configures the inter-frame gap.

```
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} inter-frame-gap bytes
```

Syntax Definitions

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.
- `bytes` Number of bytes for the inter-frame gap. Valid range is 8-31 bytes.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>12</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

```
-> interfaces port 1/1/1 inter-frame-gap 15
```

Release History

Release 8.4.1.R01; command was introduced.
**Related Commands**

*show interfaces* Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

**MIB Objects**

N/A
**interfaces flood-limit**

Configures the flood rate settings on a single port, a range of ports, or an entire Network Interface (NI).

```
interfaces {slot chassis/slot| port chassis/slot/port[-port2]} flood-limit {bcast | mcast | uucast | all} rate {pps pps_num | mbps mbps_num | cap% cap_num | enable | disable | default} [low-threshold low_num]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.
- `bcast` Specifies broadcast flood limit.
- `mcast` Specifies multicast flood limit.
- `uucast` Specifies unicast flood limit.
- `all` Specifies flood limit for all types of traffic.
- `pps_num` Packets per second.
- `mbps_num` Megabits per second.
- `cap_num` Percentage of port’s capacity.
- `enable` Enables flood rate limits.
- `disable` Disables flood rate limits.
- `default` Sets default flood rate limits.
- `low_num` Specifies the low threshold value, which must be lower than the high threshold value set for the pps_num, mbps_num, or cap_num value. 

*This parameter is not supported on the OmniSwitch 6360, 6465, 6560, 6570M, 6860N, 6900-V72/C32/X48C6/T48C6/X48C4E/X48C8, 9900 when used with the uucast parameter option.*

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide April 2023
**Usage Guidelines**

- The packets-per-second (**pps**) setting is based on a 512 byte frame size. When configuring the threshold value as a percentage (**cap%**) or in megabits-per-second (**mbps**), only approximate limits can be achieved because values are always estimated based on the packet-per-second size (512 bytes).

- The **low-threshold** parameter is set to help with the auto-recovery of a port that was shutdown because of a STORM violated state. The shutdown action is configured through the **interfaces flood-limit action** command.

**Examples**

```
-> interfaces slot 1/2 flood-limit all rate cap% 50
-> interfaces slot 1/3 flood-limit bcast rate mbps 100
-> interfaces port 1/1/1 flood-limit bcast rate mbps 60 low-threshold 40
-> interfaces port 1/1/5 flood-limit mcast rate pps 2000 low-threshold 1000
-> interfaces slot 1/1 flood-limit all rate disable
```

**Release History**

Release 7.1.1; command introduced.
Release 8.2.1; **default** and **low-threshold** parameters added.

**Related Commands**

- **show interfaces flood-rate** Displays interface flood rate settings.

**MIB Objects**

- `esmConfigTable`
  - `esmPortCfgFlow`
- `dot3PauseTable`
  - `dot3PauseAdminMode`
**interfaces flood-limit action**

Configures the action on a single port, a range of ports, when the port reaches the storm violated state.

```
interfaces {slot chassis/slot| port chassis/slot/port[-port2]} flood-limit {bcast | mcast | uucast | all} action {shutdown | trap | default}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: Slot number to configure.
- **port**: Port number of the interface to configure.
- **port2**: Last port number in a range of ports to configure.
- **bcast**: Broadcast flood limit.
- **mcast**: Multicast flood limit.
- **uucast**: Unicast flood limit. *This parameter is not supported on the OmniSwitch 6360, 6465, 6560, 6570M, 6860N, 6900-V72/C32/X48C6/T48C6/ X48C4E/X48C8, 9900.*
- **all**: Flood limit for all types of traffic.
- **shutdown**: When the high threshold is violated, port is put into a blocked state.
- **trap**: When the high threshold is crossed, trap is sent with the violation reason.
- **default**: When traffic reaches the high threshold, packets above that rate will be dropped.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When high threshold is violated, and the port needs to be put in blocked state, set the action as “shutdown”.
- Use the **low-threshold** parameter of the `interfaces flood-limit` command to assist with auto-recovery of a port that was shutdown.
- When high threshold is crossed, and a trap has to be sent with violation reason, set the action as “trap”.

• When traffic reaches high threshold, and the packets above that rate needs to be dropped, set the action as “default”.

**Examples**

-> interfaces port 1/1/1 flood-limit bcast action shutdown
-> interfaces port 1/1/4 flood uucast action trap
-> interfaces port 1/1/11 flood-limit all action shutdown
-> interfaces port 1/1/14 flood mcast action default

**Release History**

Release 8.2.1; command introduced.

**Related Commands**

- `interfaces flood-limit` Configures the high and low threshold values for flood rate limiting.
- `show interfaces flood-rate` Displays interface flood rate settings.

**MIB Objects**

- `esmConfigTable`
  - `esmPortBcastThresholdAction`
  - `esmPortMcastThresholdAction`
  - `esmPortUucastThresholdAction`
interfaces ingress-bandwidth

Configures the ingress bandwidth settings on a single port, a range of ports, or an entire Network Interface (NI).

**interfaces** {slot chassis/slot | port chassis/slot/port[-port2]} ingress-bandwidth {mbps | enable | disable}

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.
- **mbps**: Specifies the ingress bandwidth in mbps.
- **enable**: Enables ingress bandwidth limiting.
- **disable**: Disables ingress bandwidth limiting.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- -> interfaces slot 1/3 ingress-bandwidth enable
- -> interfaces slot 1/3 ingress-bandwidth mbps 30

**Release History**

Release 7.1.1; command introduced.
Related Commands

```
show interfaces ingress-rate-limit
```
Displays the ingress-rate-limit set for each interface port.

MIB Objects

```
esmConfTable
  esmPortIngressRateLimitEnable
```
interfaces pause

Configures whether or not the switch will transmit and/or honor flow control PAUSE frames on the specified interface. PAUSE frames are used to temporarily pause the flow of traffic between two connected devices to help prevent packet loss when traffic congestion occurs between switches.

`interfaces {slot chassis/slot| port chassis/slot/port[-port2]} pause {tx | rx | tx-and-rx | disable}`

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.
- `tx` Allows interface to transmit PAUSE frames to peer switches.
- `rx` Allows interface to honor PAUSE frames from peer switches and temporarily stop sending traffic to the peer.
- `tx-and-rx` Allows the interface to transmit and honor PAUSE frames to/from peer switches.
- `disable` Disables flow control on the interface.

**Defaults**

By default, flow control is disabled on all switch interfaces.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Flow control is only supported on interfaces configured to run in full-duplex mode; half-duplex mode is not supported. In addition, flow control is not supported across a virtual fabric link (VFL).
- If both autonegotiation and flow control are enabled on the same local interface, autonegotiation calculates operational flow control settings for that interface. Note that the operational settings override the configured settings as long as autonegotiation and flow control are both enabled for the interface.
- If autonegotiation is disabled, the configured flow control settings are applied to the local interface.

**Examples**

```snmp
-> interfaces port 1/2/4 pause rx
-> interfaces port 1/1/11 pause tx
```
-> interfaces port 1/2/1 pause tx-and-rx
-> interfaces port 1/2/1-6 disable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show interfaces status` Displays interface line settings.

**MIB Objects**

- `esmConfTable`
  - `esmPortCfgPause`
**interfaces link-trap**

Enables trap link messages. If enabled, a trap is generated whenever the port changes state.

```
interfaces [slot chassis/slot |  port chassis/slot/port [-port2]]  link-trap {enable | disable}
```

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.
- `enable` Port link up/down traps are displayed on the NMS.
- `disable` Port link up/down traps are not displayed on the NMS.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

- `-> interfaces port 1/2/1 link-trap enable`
- `-> interfaces slot 1/3 link-trap enable`
- `-> interfaces port 1/1/1-6 link-trap enable`

---

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

*show interfaces status*  
Displays interface line settings.

**MIB Objects**

esmConfigTable
  esmPortSlot
  esmPortIF
**interfaces ddm**

Configures the Digital Diagnostics Monitoring (DDM) administrative status.

```
interfaces ddm {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables DDM functionality.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables DDM functionality.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddm</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- DDM capability will vary based on the transceiver manufacturer.
- DDM status must be enabled in order to enable traps; traps are enabled separately.

### Examples

```
-> interfaces ddm enable
-> interfaces ddm disable
```

### Release History

Release 7.1.1; command introduced.
Related Commands

show interfaces ddm  Displays the interface DDM status.

MIB Objects

ddmConfiguration
  ddmConfig
**interfaces ddm-trap**

Configures the Digital Diagnostics Monitoring (DDM) administrative status or trap capability.

`interfaces ddm-trap {enable | disable}`

### Syntax Definitions

- **enable**: Enables DDM trap functionality.
- **disable**: Disables DDM trap functionality.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddm-trap</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

DDM status must be enabled in order to enable traps; traps are enabled separately.

### Examples

- `-> interfaces ddm-trap enable`
- `-> interfaces ddm-trap disable`

### Release History

Release 7.1.1; command introduced.

### Related Commands

- `show interfaces ddm`: Displays the interface DDM status.

### MIB Objects

- `ddmConfiguration`
- `ddmTrapConfig`
- `ddmNotificationType`
interfaces wait-to-restore

Configures the wait to restore timer on a specific slot, port, or a range of specified ports. The timer is enabled when a link up event is detected. Other applications are notified of the link up event only after the wait to restore timer has elapsed.

```
interfaces {slot chassis/slot| port chassis/slot/port|[-port2]} wait-to-restore num
```

**Syntax Definitions**

- **chassis** The chassis identifier.
- **slot** The slot number for a specific module.
- **port[-port2]** The port number. Use a hyphen to specify a range of ports.
- **num** The number of seconds the switch waits before notifying other applications. The valid range is 0-300 in multiples of 5 seconds.

**Defaults**

By default, the timer is set to zero (disabled).

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Set the wait-to-restore timer to zero to disable the timer.
- Enter a slot number to configure the timer value for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the timer value for a specific interface or a range of interfaces.

**Example**

```
-> interfaces slot 1/1 wait-to-restore 30
-> interfaces port 1/1/1 wait-to-restore 10
-> interfaces port 1/1/1-7 wait-to-restore 250
```

**Release History**

Release 7.3.2; command introduced.
Related Commands

*show interfaces* Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects

alaLinkMonConfigTable

alaLinkMonWaitToRestoreTimer
**interfaces wait-to-shutdown**

Configures the wait to shutdown timer on a specific slot, port, or a range of specified ports. The timer is enabled when a link down event is detected. Other applications are notified of the link down event only after the wait to shutdown timer has elapsed.

```
interfaces {slot chassis/slot| port chassis/slot/port[-port2]} wait-to-shutdown num
```

**Syntax Definitions**

- *chassis*  
The chassis identifier.
- *slot*  
The slot number for a specific module.
- *port[-port2]*  
The port number. Use a hyphen to specify a range of ports.
- *num*  
The number of milliseconds the switch waits before notifying other applications. The valid range is 0-300000 in multiples of 10msec.

**Defaults**

By default, the timer is set to zero (disabled).

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command can be used to reduce port flapping. If the port comes back up before the timer expires then the timer will be canceled and other applications will not be notified of the link down event.
- Set the wait-to-shutdown timer to zero to disable the timer.
- The WTS timer is not started when the switch is first booted. But administratively disabling the port will start the timer if enabled.
- The link-status of the remote port will be down when the WTS timer is running. This is due to the port being physically down and only the link-down event not being communicated to other applications.
- The WTS timer configured is the absolute value in milliseconds (i.e. if WTS value is configured as 250, then the WTS timer is set to 250 milliseconds). Timer values other than multiples of 10 (for e.g. 251) are not allowed.

**Example**

```
-> interfaces slot 1/1 wait-to-shutdown 300000
-> interfaces port 1/1/1 wait-to-shutdown 10000
```
interfaces port 1/1/1-7 wait-to-shutdown 250

Release History
Release 7.3.2; command introduced.

Related Commands
show interfaces Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

MIB Objects
alaLinkMonConfigTable
alaLinkMonWaittoShutdownTimer
**interfaces eee**

Enables or disabled Energy Efficient Ethernet.

`interfaces {slot chassis/slot| port chassis/slot/port[-port2]} eee {enable | disable}`

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.
- **enable**: Enables EEE functionality.
- **disable**: Disables EEE functionality.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- EEE is only supported on copper ports.
- Enabling EEE will start advertising EEE capability to peer ports. Disabling EEE will stop advertising EEE capability to peer ports.

**Examples**

- `-> interfaces port 1/1/1 eee enable`
- `-> interfaces slot 1/1 eee disable`

**Release History**

Release 7.3.2; command was introduced.
Related Commands

**show interfaces**
Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

**MIB Objects**

N/A
interfaces primary-port split-mode

Configures the mode of splitter cable capable ports.

`interfaces primary-port <chassis/slot/port> split-mode {auto | 4X25G | 4X10G | 40G | 100G}`

**Syntax Definitions**

- **chassis**  The chassis identifier.
- **slot**     The slot number for a specific module.
- **port**     The port number.
- **auto**     Automatically detects if a splitter cable is connected.
- **4x10g**    Sets the port to the 4X10G splitter functionality.
- **4x25g**    Sets the port to the 4X25G splitter functionality.
- **40g**      Sets the port to 40G functionality.
- **100g**     Sets the port to 100G functionality.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is only supported on ports and platforms that support the splitter cable functionality.
- The proper cable should be used based on the port’s configuration. For example, if set to 4X10G with a 40G cable connected, the port will only operate as a 10G port.
- For the OS6900-X48C6/T48C6/X48C4E/V48C8/C32E use the `interfaces port break-out` command.

**Examples**

```
-> interfaces primary-port 1/1/1 split-mode 4X10G
```
Release History

Release 7.3.4; command was introduced.
Release 8.5R2; primary-port keyword added.

Related Commands

**show interfaces split-mode**  Displays the configured and operational state of the splitter cable capable ports.

**interfaces port break-out**  Configures the mode of the splitter cable capable ports.

MIB Objects

- esmPortModeTable
- esmConfiguredMode
interfaces port break-out

Configures the break-out functionality of capable ports.

```
interfaces port {slot chassis/slot | port chassis/slot/port[-port2]} break-out {enable | disable}
```

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port/-port2**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.
- **enable**: Enables the break-out functionality.
- **disable**: Disables the break-out functionality.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- For other models, see the interfaces primary-port split-mode command.
- Perform a write memory and reload to apply the configuration.
- The following ports support the break-out functionality:
  - OS6900-T48C6 (ports 51, 54 only)
  - OS6900-X48C6 (ports 51, 54 only)
  - OS6900-X48C4E (ports 49 to 52 only)
  - OS6900-V48C8 (ports 49 to 56 only)
  - OS6900-C32E (All ports 1 to 32)
- OS6860N
  - OS68-QNI-U2 (Both ports)
  - OS68-CNI-U1

- VFL links are not supported on port configured in break-out mode.
- If break-out is disabled, both 40G and 100G transceivers are supported.
- If break-out is enabled, both 4X10 and 4X25 splitter cables are supported.
- On modules with a single link LED per port, the LED is controlled by the status of sub-port 'A' only.
- The OS68-QNI-U2 and OS68-CNI-U1 do not have additional LEDs to display the link status of break-out cables. The LED displays link status of only ports 1A and 2A respectively.
- Break-out cables cannot be auto-detected. If break-out cables are connected the break-out mode should explicitly enabled to prevent unexpected behavior such as remote link partners having a false link up.

**Examples**

-> interfaces port 1/1/1 break-out enable

**Release History**

Release 8.7R3; command was introduced.

**Related Commands**

*show interfaces break-out* Displays the break-out configuration.

*interfaces primary-port split-mode* Configures the mode of the splitter cable capable ports.

**MIB Objects**

- esmPortModeTable
- esmConfiguredMode
interfaces fec

Configures the Reed Solomon (RS-FEC) and Fire Code (FC-FEC) FEC also known as BASE-R FEC.

```
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} fec {disable | auto | fc | rs}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.
- **disable**: Disables FEC.
- **auto**: Automatically determines the FEC.
- **fc**: FC-FEC is forced.
- **rs**: RS-FEC is forced.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>fec</td>
<td>10G/40G - FC</td>
</tr>
<tr>
<td></td>
<td>25G/100G - RS</td>
</tr>
<tr>
<td></td>
<td>Direct-attached - auto (request RS-FEC and FC-FEC)</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is only supported on modules that support FEC configuration. Not supported on 1G.
- For 10G/40G FC-FEC will be requested when auto is enabled.
- For 25G/100G RS-FEC will be requested when auto is enabled.
- Beginning in 8.7R2 the default on 25G ports was changed to RS-FEC from FC-FEC.
- The OS6900-C32 does not support RS-FEC. It will be set to FC-FEC. This must be taken into account for interoperability with other models.

### Examples

```
-> interfaces port 1/1/1 fec fc
```
-> interfaces slot 1/2 fec auto

**Release History**

Release 8.4.1.R03; command was introduced.
Release 8.7R2; Default mode for 25G is RS-FEC.

**Related Commands**

- **show interfaces status** Displays the configured and operational state of the ports.

**MIB Objects**

- `esmPortModeTable`
  - `esmConfiguredMode`
**interfaces hybrid-mode**

Configures the mode of a combo port to either fiber or copper.

`interfaces {slot chassis/slot | port chassis/slot/port[-port2]} hybrid-mode {fiber | copper}`

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.
- **fiber**: Enables the fiber combo port.
- **copper**: Enables the copper combo port.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hybrid-mode</td>
<td>fiber</td>
</tr>
</tbody>
</table>

Fiber/Copper Speed       1000Mbps/auto
Fiber/Copper Duplex     Full/auto
Fiber/Copper Autoneg    Enabled/Enabled

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Each combo port can be set to either fiber or copper but not both at the same time.
- When the mode is changed on a port the speed, duplex and auto-negotiation parameters will be set to the default for that port type (see table above). Other port settings will remain the same (i.e. admin status, flood limits, alias, etc.)

---

**Examples**

- `interfaces port 1/1/9 hybrid-mode copper`
- `interfaces port 1/1/10 hybrid-mode fiber`

---

**Release History**

Release 8.6R1; command introduced.
**Related Commands**

- `interfaces speed`  
  Configures interface speed.
- `interfaces crossover`  
  Configures crossover port settings.
- `interfaces duplex`  
  Enables or disables flow (pause).
- `show interfaces status`  
  Displays interface line settings.
- `show interfaces`  
  Displays auto negotiation, speed, duplex, and crossover settings.

**MIB Objects**

- `esmConfTable`
  - `esmPortCfgHybridActiveType`
  - `esmPortCfgHybridMode`
  - `esmPortOperationalHybridType`
interfaces loopback

Enables or disables the loopback mode for the specified front-panel port. Enable the port loopback mode to support L3 VPN in-line routing for an IP over Shortest Path Bridging (SPB) configuration.

```
interfaces port chassis/slot/port[-port2] loopback
no interfaces port chassis/slot/port[-port2] loopback
```

Syntax Definitions

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.

Defaults

By default, the port loopback mode is disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to disable the port loopback mode.
- This command applies only to front-panel ports. A single port can provide the loopback function or the port can be assigned to a static link aggregate that is also configured to run in loopback mode.
- When the loopback mode is enabled, the port can be configured as a bridge and access port to provide the loopback functionality on the same port (no external cable required). However, other switch functionality is not supported on loopback ports.
- For more information about SPB L3 VPN, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

Examples

```
-> interfaces port 1/1/1 loopback
-> interfaces port 1/1/2-5 loopback
-> no interfaces port 1/1/1 loopback
```

Release History

Release 8.6R2; command introduced.
Related Commands

- **linkagg static agg loopback**: Configures a link aggregate to run in the loopback mode.
- **show interfaces status**: Displays the interface line settings (for example, speed and mode).
- **show interfaces**: Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

MIB Objects

- **alaPortXTable**
  - **alaPortXLoopbackStatus**
interfaces portgroup

Configures the speed of the ports within a port group.

`interfaces portgroup port-group-number chassis/slot/group[-group] speed [auto | 25G | 10G]`

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `group[-group]` The group number. Use a hyphen to specify a range of groups.

**Defaults**

By default, the group speed is set to `auto`.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>V48C8</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OmniSwitch 6900-V48C8 does not support a mix of 1G/10G and 25G speeds on the member ports of the same port group. Mixing 1G and 10G speeds is supported.
- Member ports of each port group are non-contiguous, use the `show interfaces portgroup` command to display the port mapping.
- 1G speed is supported when port group speed is set to either `Auto` or `10G` and the operational speed is 10G.
- When the port group speed is set to `auto` the speed of the port group is determined by the first detected transceiver on any of the member ports.

**Examples**

- `interfaces portgroup port-group-number 1/1/1 speed 25G`
- `interfaces portgroup port-group-number 1/1/2-4 speed auto`
- `interfaces portgroup port-group-number 1/1/5 speed 10G`

**Release History**

Release 8.7R2; command introduced.
Related Commands

show interfaces portgroup Displays the port group member port mapping.

MIB Objects

esmPortGroupTable
  esmPortGroupEntry
  esmPortGroupIfIndex
  esmConfiguredPortGroupSpeed
  esmOperationalPortGroupSpeed
**clear violation**

Cleans all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation. This includes applying an existing application configuration.

```
clear violation {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- **chassis**
  The chassis identifier when running in virtual chassis mode.

- **slot**
  The slot number for a specific module.

- **port[-port2]**
  The port number. Use a hyphen to specify a range of ports.

- **agg_id[-agg_id2]**
  Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When a violation is set on a physical port that is part of a link aggregate, the violation is set for the whole link aggregate. All ports on that link aggregate are brought down. When this command is applied to a link aggregate ID, all member ports of the link aggregate are activated.

- When this command is applied, all MAC addresses known to the port are cleared from the MAC address table for the switch.

**Examples**

```
-> clear violation port 1/10
-> clear violation port 2/1-5
-> clear violation linkagg 5
-> clear violation linkagg 10-20
```

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

**show violation**  
Displays the address violations that occur on ports with LPS restrictions.

**MIB Objects**

*portViolationTable*
- *portViolationClearPort*
violation recovery-maximum

Configures the maximum number of recovery attempts allowed before the port is permanently shut down. This value is configurable on a global basis (applies to all ports on all modules) and on a per-slot or per-port basis.

```
violation recovery-maximum {infinite | max_attempts}
```

```
violation [slot chassis/slot | port chassis/slot/port[-port2]] recovery-maximum {infinite | default | max_attempts}
```

Syntax Definitions

- `chassis`: The chassis identifier.
- `slot`: The slot number for a specific module.
- `port[-port2]`: The port number. Use a hyphen to specify a range of ports.
- `infinite`: Sets the recovery attempt to infinite auto recovery.
- `default`: Sets the number of recovery attempts to the global value for the specified ports. This parameter is only available when a slot, port, or range of ports is specified with this command.
- `max_attempts`: The maximum number of recovery attempts. Valid range is 0-50.

Defaults

By default, this command configures the global maximum number of recovery attempts. The global value applies to all ports on all modules in the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_attempts</td>
<td>10</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Set the maximum number of recovery attempts value to 0 to disable this recovery mechanism.
- Enter a slot number to configure the number of recovery attempts for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure the number of recovery attempts for a specific interface or a range of interfaces.
• When this command is used to configure the number of recovery attempts for all ports on a slot or for a specific port or range of ports, the value specified overrides the global maximum number of attempts configured for the switch.

• When configuring the number of recovery attempts for a specific slot, port, or range of ports, use the default parameter to reset this value to the global maximum number of attempts.

• The number of recovery attempts increments whenever a port recovers using automatic recovery timer mechanism. When the number of recovery attempts exceeds the configured threshold, the port is permanently shut down.

• Once an interface is permanently shut down, only the clear violation command can be used to recover the interface.

• The recovery mechanism tracks the number of recoveries within a fixed time window (FTW). The \( FTW = 2 \times \text{maximum recovery number} \times \text{recovery timer} \). For example, if the maximum number of recovery attempts is set to 4 and the recovery timer is set to 5, the FTW is 40 seconds \((2 \times 4 \times 5 = 40)\).

**Examples**

-> violation recovery-maximum 25
-> violation slot 1/2 recovery-maximum 10
-> violation port 1/2/3 recovery-maximum 20
-> violation port 1/2/4-9 recovery-maximum 50
-> violation port 1/2/4-9 recovery-maximum default
-> violation port 1/2/3 recovery-maximum 0
-> violation recovery-maximum infinite
-> violation recovery-maximum 0

**Release History**

Release 8.2.1; command was introduced.

**Related Commands**

- **violation recovery-time**: Configures the time interval after which the port is automatically re-activated if the port was shut down for any violation.
- **show interfaces**: Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
- **show interfaces portgroup**: Displays the globally configured recovery time, SNMP recovery trap status, and maximum recovery attempts.

**MIB Objects**

- **alaPortViolationRecoveryTable**
- **alaPortViolationRecoveryMaximum**
violation recovery-time

Configures the time interval after which the port is automatically re-activated if the port was shutdown for any violation. This value is configurable on a global basis (applies to all ports on all modules) and on a per-slot or per-port basis.

```
violation recovery-time seconds
```

```
viiolation [slot chassis/slot | port chassis/slot/port[-port2]] recovery-time {seconds | default}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of port.
- **seconds**: The number of seconds after which a port is reactivated. The valid range is 30-600 seconds.
- **default**: Sets the recovery time to the global value for the specified ports. This parameter is only available when a slot, port, or range of ports is specified with this command.

### Defaults

- By default, this command configures the global recovery time. The global value applies to all ports on all modules in the switch.
- By default, the violation recovery time is set to 300 seconds.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When the recovery timer expires, the interface is operationally re-enabled and the violation on the interface is cleared.
- The violation recovery time value does not apply to interfaces that are in a permanent shutdown state. A port in this state is only recoverable using the `clear violation` command.
- The interface violation recovery mechanism is not supported on link aggregates, but is supported on the link aggregate member ports.
- Enter a slot number to configure the recovery time for all interfaces on a specific slot.
- Enter a slot and port number or a range of ports to configure the recovery time for a specific interface or a range of interfaces.

- When this command is used to configure the recovery time for all ports on a slot or for a specific port or range of ports, the value specified overrides the global maximum recovery time configured for the switch.

- When configuring the time for a specific slot, port, or range of ports, use the `default` parameter to reset this value to the global maximum number of attempts.

**Examples**

```plaintext
-> violation recovery-time 600
-> violation slot 1/2 recovery-time 100
-> violation port 1/2/3 recovery-time 200
-> violation port 1/2/4-9 recovery-time 500
-> violation port 1/2/4-9 recovery-time default
```

**Release History**

Release 8.2.1; command introduced.

**Related Commands**

- `violation recovery-maximum` - Configures the maximum number of recovery attempts before a port is permanently shut down.
- `show violation` - Displays the violation and recovery status for the specified port.
- `show interfaces portgroup` - Displays the globally configured recovery time, SNMP recovery trap enable/disable status and maximum recovery attempts.

**MIB Objects**

- `alaPortViolationRecoveryTable`
  - `alaPortViolationRecoveryTime`
violation recovery-trap

Enables or disables the sending of a violation recovery trap when any port is re-enabled after the violation recovery time has expired.

violation recovery-trap {enable | disable}

Syntax Definitions

enable Enables the ports to send violation recovery traps.
disable Disables the ports from sending violation recovery traps.

Defaults

By default, sending of a violation recovery trap is disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This is a global command that is applied to all ports on all modules.

Examples

-> violation recovery-trap enable
-> violation recovery-trap disable

Release History

Release 8.2.1; command was introduced.
**Related Commands**

- **violation recovery-time**
  Configures the time interval to automatically re-enable the ports that were shutdown due to a violation.

- **show interfaces portgroup**
  Displays the globally configured recovery time, SNMP recovery trap status, and maximum recovery attempts.

**MIB Objects**

- *esmViolationRecovery*
  - *esmViolationRecoveryTrap*
show interfaces

Displays general interface information (for example, hardware, MAC address, input errors, and output errors).

`show interfaces [slot chassis/slot | port chassis/slot/port[-port2]]`

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot**
  - Slot number to display information about all ports on a specific slot.

- **port[-port2]**
  - The port number of a specific interface to display. Use a hyphen to specify a range of ports.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The Link-Quality parameter and Enhanced Port Performance capabilities are only supported on the OmniSwitch 6900.
- EEE will be appended to the Autonegotiation output when EEE is enabled (EEE is supported only on the OmniSwitch 6860, 6865, 6900).

### Examples

```
-> show interfaces port 1/1/2
Chassis/Slot/Port 1/1/2 :
  Operational Status : up,
  Last Time Link Changed : Mon Jan  5 17:09:30 2019,
  Number of Status Change: 1,
  Port-Down/Violation Reason: None,
  Type                   : Ethernet,
  SFP/XFP                : GBIC_SX,
  Interface Type        : Fiber,
  EPP                   : Disabled,
  Link-Quality           : Good
  MAC address            : 00:d0:95:b2:39:85,
  BandWidth (Megabits)   : 1000,                Duplex           : Full,
  Autonegotiation :  1 [ 1000-F 100-F 100-H 10-F 10-H ],
```

---

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 1-59
Long Accept : Enable,            Runt Accept : Disable,  
Long Frame Size(Bytes) : 9216,            Runt Size(Bytes) : 64,  
Inter Frame Gap(Bytes) : 12,             
loopback mode : N/A,               
Rx :          
Bytes Received :  7967624, Unicast Frames : 0,  
Broadcast Frames:  124186, M-cast Frames : 290,  
UnderSize Frames:  0, OverSize Frames: 0,  
Lost Frames : 0, Error Frames : 0,  
CRC Error Frames: 0, Alignments Err : 0,  
Tx :          
Bytes Xmitted : 255804426, Unicast Frames : 24992,  
Broadcast Frames: 3178399, M-cast Frames : 465789,  
UnderSize Frames: 0, OverSize Frames: 0,  
Lost Frames : 0, Collided Frames : 0,  
Error Frames : 0, Collisions : 0,  
Late Collisions : 0, Exc-Collisions : 0,  

output definitions

Chassis/Slot/Port  Interface chassis, slot, and port number.

Operational Status  Interface status:
  up—port is operationally up.
  down—port is operationally down
  dormant—SFP/SFP+ transceiver is inserted into a port configured for Fibre Channel or Fibre Channel transceiver in inserted into a port configured for Ethernet and the link has become active.

Last Time Link Changed  The last time the configuration for this interface was changed.

Number of Status Change  The total number of times that the configuration of this interface has changed.

Port-Down/Violation Reason  This is displayed if the port is down. If the port is down due to software reasons or violations the reason is displayed. If it is down due to physical fault, “None” is displayed. The reason displayed applies only to the physical port, for a link aggregate use the show violation command.

Type  Interface type (Ethernet/Fast Ethernet/Gigabit Ethernet).

SFP/XFP  The type of transceiver detected.

Interface Type  The type of interface for this port. (Copper, Fiber, Combo-Copper, Combo-Fiber)

EPP  Enhanced Port Performance setting.

Link-Quality  The link quality of the connection:
  GOOD—The port will connect with no problems and transfer data with no errors.
  FAIR—The port may have intermittent problems connecting and maintaining its connection to a remote port and/or intermittent CRC's could occur.
  POOR—The port will have problems connecting and maintaining a connection with remote port. If the ports connect, it’s likely CRC errors will occur.
  N/A—The port link quality is either very poor or the port type does not support the Link Quality capability.

MAC address  Interface MAC address.
### Ethernet Port Commands

**show interfaces**

---

=output definitions (continued)=

<table>
<thead>
<tr>
<th>WWPN</th>
<th>OmniSwitch 64-bit World Wide Port Name (WWPN) for each Fibre Channel port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bandwidth</td>
<td>Bandwidth (in megabits).</td>
</tr>
<tr>
<td>Duplex</td>
<td>Duplex mode (Half/Full/Auto).</td>
</tr>
<tr>
<td>Autonegotiation</td>
<td>The auto negotiation settings for this interface.</td>
</tr>
<tr>
<td>Long Accept</td>
<td>Long Frames status (enable/disable).</td>
</tr>
<tr>
<td>Runt Accept</td>
<td>Runt Frames status (enable/disable).</td>
</tr>
<tr>
<td>Long Frame Size</td>
<td>Long Frame Size (in Bytes).</td>
</tr>
<tr>
<td>Runt Size</td>
<td>Runt Frame Size (in Bytes).</td>
</tr>
<tr>
<td>Inter Frame Gap</td>
<td>Inter-packet gap (in Bytes).</td>
</tr>
<tr>
<td>loopback mode</td>
<td>The loopback mode for the port (N/A or SPB-VPN). Ports are configured to run in the loopback mode to support L3 VPN in-line routing for an IP over Shortest Path Bridging (SPB) configuration.</td>
</tr>
<tr>
<td>Bytes Received</td>
<td>Number of Bytes received.</td>
</tr>
<tr>
<td>Rx Unicast Frames</td>
<td>Number of unicast frames received.</td>
</tr>
<tr>
<td>Rx Broadcast Frames</td>
<td>Number of broadcast frames received.</td>
</tr>
<tr>
<td>Rx M-cast Frames</td>
<td>Number of multicast frames received.</td>
</tr>
<tr>
<td>Rx Undersize Frames</td>
<td>Number of undersized frames received.</td>
</tr>
<tr>
<td>Rx Oversize Frames</td>
<td>Number of oversized frames received.</td>
</tr>
<tr>
<td>Rx Lost Frames</td>
<td>Number of Lost Frames received.</td>
</tr>
<tr>
<td>Rx Error Frames</td>
<td>Number of error frames received.</td>
</tr>
<tr>
<td>Rx CRC Error Frames</td>
<td>Number of CRC error frames received. Only applies to frames that are less than or equal to Max/Long Frame Size. Frames larger than Long Frame Size are counted as OverSizeFrames.</td>
</tr>
<tr>
<td>Rx Alignments Err</td>
<td>Number of Alignments Error frames received.</td>
</tr>
<tr>
<td>Bytes Xmitted</td>
<td>Number of Bytes transmitted.</td>
</tr>
<tr>
<td>Tx Unicast Frames</td>
<td>Number of unicast frames transmitted.</td>
</tr>
<tr>
<td>Tx Broadcast Frames</td>
<td>Number of broadcast frames transmitted.</td>
</tr>
<tr>
<td>Tx M-cast Frames</td>
<td>Number of multicast frames transmitted.</td>
</tr>
<tr>
<td>Tx Undersize Frames</td>
<td>Number of undersized frames transmitted.</td>
</tr>
<tr>
<td>Tx Oversize Frames</td>
<td>Number of oversized frames transmitted.</td>
</tr>
<tr>
<td>Tx Lost Frames</td>
<td>Number of Lost Frames transmitted.</td>
</tr>
<tr>
<td>Tx Collided Frames</td>
<td>Number of collision frames received or transmitted.</td>
</tr>
<tr>
<td>Tx Error Frames</td>
<td>Number of error frames transmitted.</td>
</tr>
<tr>
<td>Collisions</td>
<td>Number of single collisions.</td>
</tr>
<tr>
<td>Late Collisions</td>
<td>Number of late collisions.</td>
</tr>
<tr>
<td>Exc-Collisions</td>
<td>Number of excessive collisions.</td>
</tr>
</tbody>
</table>


**Release History**
Release 7.1.1; command introduced.
Release 8.6R2; “Port-Down Reason/Violation Reason”, “Interface Type”, and “loopback mode” output fields added.

**Related Commands**
- `show interfaces accounting`: Displays interface accounting information (e.g., packets received/transmitted).
- `show interfaces counters`: Displays interface counter information (e.g., unicast packets received/transmitted).
- `show interfaces status`: Displays the interface line settings (e.g., speed and mode).
- `show interfaces traffic`: Displays interface traffic statistics (input/output bytes and packets).

**MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifTable</td>
<td></td>
</tr>
<tr>
<td>ifOperStatus</td>
<td></td>
</tr>
<tr>
<td>ifType</td>
<td></td>
</tr>
<tr>
<td>ifPhysAddress</td>
<td></td>
</tr>
<tr>
<td>ifSpeed</td>
<td></td>
</tr>
<tr>
<td>ifInDiscards</td>
<td></td>
</tr>
<tr>
<td>ifOutDiscards</td>
<td></td>
</tr>
<tr>
<td>esmConfTable</td>
<td></td>
</tr>
<tr>
<td>esmPortSlot</td>
<td></td>
</tr>
<tr>
<td>esmPortIF</td>
<td></td>
</tr>
<tr>
<td>esmPortCfgLongEnable</td>
<td></td>
</tr>
<tr>
<td>esmPortCfgRuntEnable</td>
<td></td>
</tr>
<tr>
<td>esmPortCfgMaxFrameSize</td>
<td></td>
</tr>
<tr>
<td>esmPortCfgRuntSize</td>
<td></td>
</tr>
<tr>
<td>esmPortDownReason</td>
<td></td>
</tr>
<tr>
<td>esmPortInterfaceType</td>
<td></td>
</tr>
<tr>
<td>alaPortXTable</td>
<td></td>
</tr>
<tr>
<td>alaPortXLoopbackStatus</td>
<td></td>
</tr>
<tr>
<td>ifXTable</td>
<td></td>
</tr>
<tr>
<td>ifHCInOctets</td>
<td></td>
</tr>
<tr>
<td>ifHCInUcastPkts</td>
<td></td>
</tr>
<tr>
<td>ifHCinBroadcastPkts</td>
<td></td>
</tr>
<tr>
<td>ifHCInMulticastPkts</td>
<td></td>
</tr>
<tr>
<td>IfHCOutOctets</td>
<td></td>
</tr>
<tr>
<td>IfHCOutUcastPkts</td>
<td></td>
</tr>
<tr>
<td>IfHCOutBroadcastPkts</td>
<td></td>
</tr>
<tr>
<td>IfHCOutMulticastPkts</td>
<td></td>
</tr>
<tr>
<td>alcetherStatsTable</td>
<td></td>
</tr>
<tr>
<td>alcetherStatsRxUndersizePkts</td>
<td></td>
</tr>
<tr>
<td>alcetherStatsCRCAlignErrors</td>
<td></td>
</tr>
<tr>
<td>alcetherStatsTxUndersizePkts</td>
<td></td>
</tr>
<tr>
<td>alcetherStatsTxOversizePkts</td>
<td></td>
</tr>
<tr>
<td>alcetherStatsTxCollisions</td>
<td></td>
</tr>
<tr>
<td>dot3StatsTable</td>
<td></td>
</tr>
<tr>
<td>dot3StatsFrameTooLong</td>
<td></td>
</tr>
<tr>
<td>dot3StatsFCSErrors</td>
<td></td>
</tr>
<tr>
<td>dot3StatsLateCollisions</td>
<td></td>
</tr>
</tbody>
</table>
**show interfaces alias**

Displays interface line settings (e.g., speed and mode).

```
show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] alias
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: Slot number to display information about all ports on a specific slot.
- **port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.

### Examples

```
-> show interfaces port 1/1/2 alias
Legends: WTS - Wait to shutdown
# - WTS Timer is Running & port is in wait-to-shutdown state

Chas/Slot/Port Admin Link WTR WTS Alias
-----+----------+---------+-----+----+----------------------------------
1/1/2  disable  down  5  #10  ""
```

### output definitions

- **Chas/Slot/Port**: Interface chassis/slot/port number.
- **Admin Status**: The administrative status of the port.
- **Link Status**: The link status of the port. Autonegotiation status (Enable/Disable).
- **WTS (msec)**: The wait-to-shutdown configuration time.
output definitions (continued)

| WTR (sec) | The wait-to-restore configuration time. |
| Alias     | The configured alias for the port.     |

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **interfaces alias**
  Configures the port alias.

**MIB Objects**

- **ifXTable**
  - **ifAlias**
show interfaces status

Displays interface line settings (for example, speed and mode).

```
show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] status
```

**Syntax Definitions**

- **chassis** The chassis identifier.
- **slot** Slot number to display information about all ports on a specific slot.
- **port[-port2]** The port number of a specific interface to display. Use a hyphen to specify a range of ports.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no slot/port numbers are entered, line settings for all slots/ports on the switch are displayed.

**Examples**

```
-> show interfaces status

Slot/ Port    Admin Status Nego  DETECTED-VALUES  CONFIGURED-VALUES
  Chas/Slot  |  Speed  Duplex Resume  |  Speed  Duplex Resume
            |  (Mbps)  |               |  (Mbps)  |               |
--------+----------------+-------------------------------+----------------+-------------------------------
1/1/1A   | 40000 | Full | AUTO | en | dis
1/1/1B   | 1000  | Full | AUTO | en | dis
1/1/1C   | 1000  | Full | AUTO | en | dis
1/1/1D   | 1000  | Full | AUTO | en | dis
1/1/2A   | 40000 | Full | AUTO | en | dis
1/1/2B   | 1000  | Full | AUTO | en | dis
1/1/2C   | 1000  | Full | AUTO | en | dis
1/1/2D   | 1000  | Full | AUTO | en | dis
1/3/1    | 1000  | Full | AUTO | en | dis
1/3/2    | 1000  | Full | AUTO | en | dis
1/3/3    | 1000  | Full | AUTO | en | dis
1/3/4    | 1000  | Full | AUTO | en | dis
1/3/5    | 1000  | Full | AUTO | en | dis
```
-> show interfaces port 1/3/1 status

<table>
<thead>
<tr>
<th>Slot/Chas/Port</th>
<th>DETECTED-VALUES</th>
<th>CONFIGURED-VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot/Port</td>
<td>Status</td>
<td>Nego</td>
</tr>
<tr>
<td>----------------</td>
<td>------------------</td>
<td>------</td>
</tr>
<tr>
<td>1/3/1</td>
<td>en</td>
<td>dis</td>
</tr>
</tbody>
</table>

**output definitions**

- **Chas/Slot/Port**: Interface chassis/slot/port number.
- **Admin Status**: The administrative status of the port. Configured through the `interfaces` command.
- **AutoNego**: Autonegotiation status (Enable/Disable). Configured through the `interfaces` command.
- **Detected Speed**: Detected line speed in Mbps.
- **Detected Duplex**: Detected line duplex (Half duplex/Full duplex/Auto).
- **Detected Pause**: Detected pause control configuration.
- **FEC Det**: The detected FEC settings (DIS, FC, RS).
- **Configured Speed**: Configured line speed (10/100/Auto/1000/10000 Mbps). Configured through the `interfaces speed` command.
- **Configured Duplex**: Configured line duplex (Half duplex/Full duplex/Auto). Configured through the `interfaces duplex` command.
- **FEC Cfg**: The configured FEC settings (Disable, Auto, FC, RS).
- **Configured Pause**: Detected pause control configuration. Configured through the `interfaces pause` command.
- **Link Trap**: Link Trap status. Configured through the `interfaces link-trap` command.
- **EEE**: Energy Efficient Ethernet configuration (dis/ena).

**Release History**

Release 7.1.1; command introduced.
Release 8.4.1.R03; **FEC Det** and **FEC Cfg** fields added.

**Related Commands**

- **interfaces**: Configures interface line speed, sets speed, and duplex mode to auto-sensing.
- **interfaces duplex**: Configures interface duplex mode.
- **interfaces fec**: Configures the Reed Solomon (RS-FEC) and Fire Code (FC-FEC) FEC also known as BASE-R FEC.
**MIB Objects**

- esmConfTable
  - esmPortSlot
  - esmPortIF
  - esmPortAutoSpeed
  - esmPortAutoDuplexMode
  - esmPortCfgAutoNegotiation
  - esmPortCfgSpeed
  - esmPortCfgDuplexMode
  - esmPortCfgPause
  - esmPortLinkUpDownTrapEnable
show interfaces capability

Displays default auto negotiation, speed, duplex, flow, and cross-over settings for a single port, a range of ports, or all ports on a Network Interface (NI) module.

```
show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] capability
```

Syntax Definitions

- **chassis**: The chassis identifier when running in virtual chassis mode.
- **slot**: Slot number to display information about all ports on a specific slot.
- **port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Displays defaults settings in two rows of data for each port. The first row of data, identified by the label **CAP**, displays the valid user-defined configuration settings available for the port. The second row, identified by the label **DEF**, displays the default settings for the port.

Examples

```
-> show interfaces capability
```

<table>
<thead>
<tr>
<th>Ch/Slot/Port</th>
<th>AutoNeg</th>
<th>Pause</th>
<th>Crossover</th>
<th>Speed</th>
<th>Duplex</th>
<th>Macsec Supported</th>
<th>Macsec 256-bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>CAP</td>
<td>EN/DIS</td>
<td>Tx/Rx/Tx&amp;Rx/DIS</td>
<td>MDI/X/Auto</td>
<td>10/100/1G</td>
<td>Full/Half</td>
<td>NO</td>
</tr>
<tr>
<td>1/1/1</td>
<td>DEF</td>
<td>EN</td>
<td>DIS</td>
<td>Auto</td>
<td>Auto</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>1/1/2</td>
<td>CAP</td>
<td>EN/DIS</td>
<td>Tx/Rx/Tx&amp;Rx/DIS</td>
<td>MDI/X/Auto</td>
<td>10/100/1G</td>
<td>Full/Half</td>
<td>NO</td>
</tr>
<tr>
<td>1/1/2</td>
<td>DEF</td>
<td>EN</td>
<td>DIS</td>
<td>Auto</td>
<td>Auto</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>1/1/3</td>
<td>CAP</td>
<td>EN/DIS</td>
<td>Tx/Rx/Tx&amp;Rx/DIS</td>
<td>MDI/X/Auto</td>
<td>10/100/1G</td>
<td>Full/Half</td>
<td>NO</td>
</tr>
<tr>
<td>1/1/3</td>
<td>DEF</td>
<td>EN</td>
<td>DIS</td>
<td>Auto</td>
<td>Auto</td>
<td>Auto</td>
<td>Auto</td>
</tr>
<tr>
<td>1/1/25</td>
<td>CAP</td>
<td>DIS</td>
<td>Tx/Rx/Tx&amp;Rx/DIS</td>
<td>-</td>
<td>10G</td>
<td>Full</td>
<td>YES</td>
</tr>
<tr>
<td>1/1/25</td>
<td>DEF</td>
<td>DIS</td>
<td>DIS</td>
<td>-</td>
<td>10G</td>
<td>Full</td>
<td>YES</td>
</tr>
<tr>
<td>1/1/26</td>
<td>CAP</td>
<td>DIS</td>
<td>Tx/Rx/Tx&amp;Rx/DIS</td>
<td>-</td>
<td>10G</td>
<td>Full</td>
<td>YES</td>
</tr>
<tr>
<td>1/1/26</td>
<td>DEF</td>
<td>DIS</td>
<td>DIS</td>
<td>-</td>
<td>10G</td>
<td>Full</td>
<td>NO</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Cha/Slot/Port</th>
<th>The chassis/slot/port identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AutoNeg</strong></td>
<td>In the row labeled <strong>CAP</strong>, the field displays the valid auto negotiation configurations for the port. In the row label <strong>DEF</strong>, the field displays the default auto negotiation settings for the port. The possible values are <strong>EN</strong> (enabled) or <strong>DIS</strong> (disabled).</td>
</tr>
<tr>
<td><strong>Pause</strong></td>
<td>In the row labeled <strong>CAP</strong>, the field displays the valid pause configurations for the port. In the row label <strong>DEF</strong>, the field displays the default pause settings for the port.</td>
</tr>
<tr>
<td><strong>Crossover</strong></td>
<td>In the row labeled <strong>CAP</strong>, the field displays the valid cross over configurations for the port. In the row label <strong>DEF</strong>, the field displays the default cross over settings for the port. The possible values are <strong>Auto</strong>, <strong>MDI/X/Auto</strong> (MDI/MDIX/Auto), or <strong>--</strong> (not configurable and/or not applicable).</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>In the row labeled <strong>CAP</strong>, the field displays the valid line speed configurations for the port. In the row label <strong>DEF</strong>, the field displays the default line speed settings for the port. The possible values are <strong>10/100</strong>, <strong>100</strong>, <strong>1G</strong>, <strong>10/100/1G</strong>, <strong>10G</strong>, or <strong>Auto</strong>.</td>
</tr>
<tr>
<td><strong>Duplex</strong></td>
<td>In the row labeled <strong>CAP</strong>, the field displays the valid duplex configurations for the port. In the row label <strong>DEF</strong>, the field displays the default duplex settings for the port. The possible values are <strong>Full</strong>, <strong>Full/Half</strong>, or <strong>Auto</strong>.</td>
</tr>
<tr>
<td><strong>Macsec Supported</strong></td>
<td>Indicates if the interface has support for MACsec 128-bit encryption.</td>
</tr>
<tr>
<td><strong>Macsec 256-bit</strong></td>
<td>Indicates if the interface has support for MACsec 256-bit encryption.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 8.5 R1; **Macsec Supported** field added.
Release 8.7R1; **Macsec 256-bit** field added.

**Related Commands**

- **interfaces** Enables and disables auto negotiation.
- **interfaces crossover** Configures crossover port settings.
- **interfaces** Configures interface speed.
- **interfaces duplex** Configures duplex settings.
- **show interfaces alias** Displays interface line settings.

**MIB Objects**

- **esmConfTable**
  - **esmPortCfgAutoNegotiation**
  - **esmPortCfgFlow**
  - **esmPortCfgCrossover**
  - **esmPortCfgSpeed**
  - **esmPortAutoDuplexMode**
**show interfaces accounting**

Displays interface accounting information (e.g., packets received/transmitted and deferred frames received).

```
show interfaces [slot chassis[slot | port chassis[slot/port][-port2]]] accounting
```

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: Slot number to display information about all ports on a specific slot.
- **slot/port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If no slot/port numbers are entered, accounting information for all slots/ports on the switch is displayed.
- The OmniSwitch 9900 supports different packet size ranges than the other OmniSwitch platforms. All packets sized 1024 octets or larger are classified into the “1024 to MAX” category. As a result, this command displays a different output on the OmniSwitch 9900.

**Examples**

The following command example shows the fields that are displayed on all OmniSwitch platforms, except for the OmniSwitch 9900:

```
-> show interfaces accounting
1/1/39:
  Rx Undersize = 0, Tx Undersize = 0,
  Rx Oversize = 0, Tx Oversize = 0,
  Rx Jabber = 0,
  Rx/Tx 64 Octets = 312890503,
  Rx/Tx 65 ~ 127 Octets = 10496825,
  Rx/Tx 128 ~ 255 Octets = 189426,
  Rx/Tx 256 ~ 511 Octets = 39328,
  Rx/Tx 512 ~ 1023 Octets = 756,
```
The following command example shows the fields that are displayed on an OmniSwitch 9900 (the “Rx/Tx 1024 - MAX Octets” field replaces the “Rx/Tx 1024 - 1518 Octets”, “Rx/Tx 1519 - 4095 Octets”, and “Rx/Tx 4096 - MAX Octets” fields that are displayed on the other platforms:

```
-> show interfaces accounting
1/4/38:
  Rx Undersize              =               0, Tx Undersize =               0,
  Rx Oversize               =               0, Tx Oversize =               0,
  Rx Jabber                 =               0,
  Rx/Tx 64 Octets           =            361616757,
  Rx/Tx 65 ~ 127 Octets     =             20510941,
  Rx/Tx 128 ~ 255 Octets    =               377413,
  Rx/Tx 256 ~ 511 Octets    =               45391,
  Rx/Tx 512 ~ 1023 Octets   =               2319,
  Rx/Tx 1024 ~ MAX Octets   =              63555,
```

**output definitions**

- **Rx Undersize**: Number of undersized packets received.
- **Tx Undersize**: Number of undersized packets transmitted.
- **Rx oversize**: Number of oversized packets received.
- **Tx oversize**: Number of oversized packets transmitted.
- **Rx Jabber**: Number of Jabber packets received (longer than 1518 octets).
- **Rx/Tx Octets**: Number of packets received and transmitted in each listed octet range.

**Release History**

Release 7.1.1; command introduced.
Release 8.3.1; display updated for OmniSwitch 9900.

**Related Commands**

- **interfaces ddm**: Displays general interface information (e.g., hardware, MAC address, and input/output errors).
- **show interfaces counters**: Displays interface counter information (e.g., unicast packets received/transmitted).
**MIB Objects**

`esmConfTable`
- `esmPortSlot`
- `esmPortIF`

`dot3StatsTable`
- `dot3StatsFrameTooLong`
- `dot3StatsDeferredTransmissions`

`alcetherStatsTable`
- `alcetherStatRxsUndersizePkts`
- `alcetherStatTxsUndersizePkts`
- `alcetherStatsTxOversizePkts`
- `alcetherStatsPkts64Octets`
- `alcetherStatsPkts65to127Octets`
- `alcetherStatsPkts128to255Octets`
- `alcetherStatsPkts256to511Octets`
- `alcetherStatsPkts512to1023Octets`
- `alcetherStatsPkts1024to1518Octets`
- `gigaEtherStatsPkts1519to4095Octets`
- `gigaEtherStatsPkts4096to9215Octets`
- `alcetherStatsRxJabber`
show interfaces counters

Displays interface counters information (e.g., unicast, broadcast, and multi-cast packets received/transmitted).

show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] counters

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: Slot number to display information about all ports on a specific slot.
- **port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If no slot/port numbers are entered, counter information for all slots/ports on the switch is displayed.

Examples

```
-> show interfaces port 1/3/1 counters
1/3/1,
InOctets   = 5436757858697979, OutOctets = 5.78E19,
InUcastPkts= 55654265276, OutUcastPkts = 5.78E20,
InMcastPkts= 5876786786768777, OutMcastPkts = 5465758756856,
InBcastPkts= 576567567567567576, OutBcastPkts = 786876,
InPauseFrames = 567798768768767, OutPauseFrames= 786876,
```

**output definitions**

- **InOctets**: Number of octets received.
- **OutOctets**: Number of octets transmitted.
- **InUcastPkts**: Number of unicast packets received.
- **OutUcastPkts**: Number of unicast packets transmitted.
- **InMcastPkts**: Number of multicast packets received.
- **OutMcastPkts**: Number of unicast packets transmitted.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InBcastPkts</td>
<td>Number of broadcast packets received.</td>
</tr>
<tr>
<td>OutBcastPkts</td>
<td>Number of unicast packets transmitted.</td>
</tr>
<tr>
<td>InPauseFrames</td>
<td>Number of MAC control frames received.</td>
</tr>
<tr>
<td>OutPauseFrames</td>
<td>Number of MAC control frames transmitted.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**show interfaces counters errors**

Displays interface error frame information (e.g., CRC errors, transit errors, and receive errors).

**MIB Objects**

- esmConfTable
  - esmPortSlot
  - esmPortIF
- ifXTable
  - IfHCInOctets
  - IfHCOutOctets
  - IfHCInUcastPkts
  - IfHCOutUcastPkts
  - IfHCInMulticastPkts
  - IfHCOutMulticastPkts
  - IfHCInBroadcastPkts
  - IfHCOutBroadcastPkts
- dot3PauseTable
  - dot3InPauseFrame
  - dot3OutPauseFrame
show interfaces counters errors

Displays interface error frame information (e.g., CRC errors, transit errors, and receive errors).

show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] counters errors

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: Slot number to display information about all ports on a specific slot.
- **port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no slot/port numbers are entered, counter error information for all slots/ports on the switch is displayed.

**Examples**

```
-> show interfaces port 1/2/1 counters errors
1/2/1,
   Alignments Errors = 6.45E13,  FCS Errors = 7.65E12
   IfInErrors      = 6435346,  IfOutErrors = 5543,
   Undersize pkts  = 867568,  Oversize pkts = 5.98E8
```

**output definitions**

- **Chas/Slot/Port**: Interface chassis, slot, and port number.
- **Alignments Errors**: Number of Alignments errors.
- **FCS Errors**: Number of Frame Check Sequence errors.
- **IfInErrors**: Number of received error frames.
- **IfOutErrors**: Number of transmitted error frames.
- **Undersize pkts**: Number of undersized packets.
- **Oversize pkts**: Number of oversized packets (more than 1518 octets).
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`show interfaces counters` Displays interface counters information (e.g., unicast, broadcast, and multi-cast packets received/transmitted).

**MIB Objects**

- `esmConfTable`
  - `esmPortSlot`
  - `esmPortIF`
- `ifTable`
  - `ifInErrors`
  - `ifOutErrors`
- `alcetherStatsTable`
  - `alcetherStatsRxUndersizePkts`
- `dot3StatsTable`
  - `dot3StatsAlignmentErrors`
  - `dot3StatsFCSErrors`
  - `dot3StatsFrameTooLong`
**show interfaces flood-rate**

Displays interface peak flood rate settings.

```
show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] flood-rate [bcast | mcast | uucast]
```

**Syntax Definitions**

- `chassis`     The chassis identifier.
- `slot`        Slot number to display information about all ports on a specific slot.
- `port[-port2]` The port number of a specific interface to display. Use a hyphen to specify a range of ports.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show interfaces flood-rate
Chas/
Slot/ Port Value Type Status Value Type Status Value Type Status
------------------------------
1/1/1 496 mbps enable 496 mbps enable 496 mbps disable
1/1/2 496 mbps enable 496 mbps enable 496 mbps disable
1/1/3 496 mbps enable 496 mbps enable 496 mbps disable
1/1/4 496 mbps enable 496 mbps enable 496 mbps disable
1/1/5 496 mbps enable 496 mbps enable 496 mbps disable
```

**output definitions**

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Value</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface slot and port numbers.</td>
<td>The value set based on the type of flood limiting.</td>
<td>The type of flood limiting: mbps, pps, or %</td>
<td>Status of the type of flood-limiting: enabled or disabled.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

```
interfaces flood-limit
```

Configures the peak flood rate for an interface.

**MIB Objects**

```
esmConfTable
  esmPortSlot
  esmPortIF
  esmPortMaxFloodRate
  esmPortFloodMcastEnable
```
show interfaces traffic

Displays interface traffic statistics.

`show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] traffic`

**Syntax Definitions**

- `chassis` The chassis identifier when running in virtual chassis mode.
- `slot` Slot number to display information about all ports on a specific slot.
- `port[-port2]` The port number of a specific interface to display. Use a hyphen to specify a range of ports.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no slot/port numbers are entered, traffic settings for all slots/ports on the switch are displayed.

**Examples**

```
-> show interfaces traffic
Ch/Slot/Port   Input packets     Input bytes      Output packets    Output bytes
-------------+-----------------+-----------------+-----------------+---------------
1/1/2                322             20624              5125            347216
1/3/2                322             20620              5133            347764
```

**output definitions**

- **Ch/Slot/Port** Interface chassis, slot, and port numbers.
- **Input packets** Input packets detected.
- **Input bytes** Input bytes detected.
- **Output packets** Output packets detected.
- **Output bytes** Output bytes detected.
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **interfaces ddm**
  Displays general interface information (e.g., hardware, MAC address, and input/output errors).

- **show interfaces counters**
  Displays interface counter information (e.g., unicast packets received/transmitted).

**MIB Objects**

- **esmConfTable**
  - **esmPortSlot**
  - **esmPortIF**

- **ifXTable**
  - **ifHCInOctets**
  - **ifHCInUcastPkts**
  - **ifHCInMulticastPkts**
  - **ifHCInBroadcastPkts**
  - **ifHCOutOctets**
  - **ifHCOutUcastPkts**
  - **ifHCOutMulticastPkts**
  - **ifHCOutBroadcastPkts**
**show interfaces ingress-rate-limit**

Displays the ingress-rate-limit set for each interface port.

```
show interfaces [slot chassis/slot| port chassis/slot/port[-port]] ingress-rate-limit
```

**Syntax Definitions**

- **chassis**  
  The chassis identifier.

- **slot**  
  Slot number to display information about all ports on a specific slot.

- **port[-port]**  
  The port number of a specific interface to display. Use a hyphen to specify a range of ports.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

If the slot number is not specified, then the switch back pressure feature must be enabled or disabled on an entire chassis.

**Examples**

```
-> show interfaces port 1/1/1-4 ingress-rate-limit
Chas/Slot/Port     Rate Limit (Mbps)     Burst Size (MB)     Status
1/1/1               496                 19                disable
1/1/2               496                 19                disable
1/1/3               496                 19                disable
1/1/4               496                 19                disable
```

**output definitions**

- **Chas/Slot/Port**  
  Interface chassis, slot, and port numbers.

- **Rate Limit (Mbps)**  
  Rate limit in Megabits.

- **Burst Size (MB)**  
  Burst size in Megabytes.

- **Status**  
  Status of rate limiting.
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`show interfaces ingress-rate-limit` Configures the ingress-rate-limit.

**MIB Objects**

- `esmConfTable`
- `esmPortSlot`
- `esmPortIP`
**show interfaces ddm**

Displays the Digital Diagnostics Monitoring (DDM) information for the specified transceivers.

```
show interfaces [slot chassis/slot| port chassis/slot/port[-port1]] ddm [w-low | w-high | status | a-low | a-high | actual]
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: Display all the transceivers on the specified slot.
- **port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.
- **w-low**: Display the transceivers Warning Low value.
- **w-high**: Display the transceivers Warning High value.
- **status**: Display the administrative status of DDM.
- **a-low**: Display the transceivers Alarm Low value.
- **a-high**: Display the transceivers Alarm High value.
- **actual**: The real-time values indicated by the transceiver. Values displayed in parentheses indicate the Warning or Alarm value that has been reached.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If the threshold values of the transceiver are ‘0’ then NS (Not Supported) will be displayed in the DDM output display.

### Examples

```
-> show interfaces ddm w-low
Chas/Slot/Port Temp (C) Voltage (V) Tx Bias (mA) Output (dBm) Input (dBm)
------------------------------------------------------------------------------------
 1/1    48    5.15    50    2.50    2.50
 1/2    47    5.35    49    2.43    2.43
 1/3  NA  NA  NA  NA  NA
```
Ethernet Port Commands

-> show interfaces ddm a-high

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Temp (C)</th>
<th>Voltage (V)</th>
<th>Tx Bias (mA)</th>
<th>Output (dBm)</th>
<th>Input (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>50</td>
<td>5.75</td>
<td>75</td>
<td>3.22</td>
<td>3.22</td>
</tr>
<tr>
<td>1/1/2</td>
<td>50</td>
<td>5.95</td>
<td>65</td>
<td>3.22</td>
<td>3.22</td>
</tr>
<tr>
<td>1/1/3</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

-> show interfaces port 1/1/1 ddm

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Thres-hold</th>
<th>Temp (C)</th>
<th>Voltage (V)</th>
<th>Tx Bias (mA)</th>
<th>Output (dBm)</th>
<th>Input (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Actual</td>
<td>50</td>
<td>1.95 (WL)</td>
<td>75</td>
<td>4.92 (AH)</td>
<td>3.22</td>
</tr>
<tr>
<td></td>
<td>Alarm High</td>
<td>120</td>
<td>5.75</td>
<td>100</td>
<td>4.91</td>
<td>4.91</td>
</tr>
<tr>
<td></td>
<td>Warning High</td>
<td>90</td>
<td>3.00</td>
<td>90</td>
<td>4.77</td>
<td>4.77</td>
</tr>
<tr>
<td></td>
<td>Warning Low</td>
<td>10</td>
<td>2.00</td>
<td>60</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td></td>
<td>Alarm Low</td>
<td>-5</td>
<td>1.75</td>
<td>20</td>
<td>-3.01</td>
<td>-10</td>
</tr>
</tbody>
</table>

-> show interfaces ddm status

DDM Status : enable
DDM Trap Status : disable

output definitions

<table>
<thead>
<tr>
<th>Chas/Slot/Port</th>
<th>Interface chassis, slot, and port numbers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temp C</td>
<td>The transceiver temperature, in degrees centigrade.</td>
</tr>
<tr>
<td>Voltage (V)</td>
<td>The transceiver supply voltage, in volts.</td>
</tr>
<tr>
<td>Tx Bias (mA)</td>
<td>The transceiver transmit bias current, in milliamps.</td>
</tr>
<tr>
<td>Output (dBm)</td>
<td>The transceiver output power, in decibels.</td>
</tr>
<tr>
<td>Input (dBm)</td>
<td>The transceiver received optical power, in decibels.</td>
</tr>
<tr>
<td>N/A</td>
<td>Indicates the transceiver does support DDM.</td>
</tr>
<tr>
<td>N/S</td>
<td>Indicates the transceiver does not support the DDM attribute.</td>
</tr>
<tr>
<td>Actual</td>
<td>The real-time values indicated by the transceiver. Values displayed in parentheses indicate the Warning or Alarm value that has been reached.</td>
</tr>
<tr>
<td>Alarm High (AH)</td>
<td>Indicates the value at which the transceiver’s functionality may be affected.</td>
</tr>
<tr>
<td>Warning High (WH)</td>
<td>Indicates the transceiver is approaching the High Alarm value.</td>
</tr>
<tr>
<td>Warning Low (WL)</td>
<td>Indicates the transceiver is approaching the Low Alarm value.</td>
</tr>
<tr>
<td>Alarm Low (AL)</td>
<td>Indicates the value at which the transceiver’s functionality may be affected.</td>
</tr>
<tr>
<td>DDM Status</td>
<td>The administrative status of DDM.</td>
</tr>
<tr>
<td>DDM Trap Status</td>
<td>The administrative status of DDM traps.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Related Commands

**interfaces ddm**

Configures the DDM administrative status or trap capability.

MIB Objects

ddmNotifications

- ddmTemperature
- ddmTempLowWarning
- ddmTempLowAlarm
- ddmTempHiWarning
- ddmTempHiAlarm
- ddmSupplyVoltage
- ddmSupplyVoltageLowWarning
- ddmSupplyVoltageLowAlarm
- ddmSupplyVoltageHiWarning
- ddmSupplyVoltageHiAlarm
- ddmTxBiasCurrent
- ddmTxBiasCurrentLowWarning
- ddmTxBiasCurrentLowAlarm
- ddmTxBiasCurrentHiWarning
- ddmTxBiasCurrentHiAlarm
- ddmTxOutputPower
- ddmTxOutputPowerLowWarning
- ddmTxOutputPowerLowAlarm
- ddmTxOutputPowerHiWarning
- ddmTxOutputPowerHiAlarm
- ddmRxOpticalPower
- ddmRxOpticalPowerLowWarning
- ddmRxOpticalPowerLowAlarm
- ddmRxOpticalPowerHiWarning
- ddmRxOpticalPowerHiAlarm
**show interfaces split-mode**

Displays the configured and operational state of the 4X10G capable ports.

```
show interfaces [slot chassis/slot | port chassis/slot/port[-port1]] split-mode
```

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` Display all the ports on the specified slot.
- `port[-port2]` The port number of a specific interface to display. Use a hyphen to specify a range of ports.

---

**Defaults**

By default, information for all ports that support the splitter cable functionality is displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The output is only displayed for those ports that support the splitter cable functionality.

---

**Examples**

```
-> show interfaces split-mode
Ch/Slot/Primary-Port  Split-Mode Configured Operational Member-Port
-----------------------------------------------
1/1/1A                4X10         4X10G     1/1/1A-1/1/1D
1/1/2A                AUTO         40G       1/1/2A-1/1/2D
1/1/3A                40G          40G       1/1/3A-1/1/3D
1/1/4A                AUTO         None      1/1/4A-1/1/4D
<output truncated>
```

---

**output definitions**

- **Ch/Slot/Port** The chassis, slot, and port.
Output Definitions (continued)

<table>
<thead>
<tr>
<th>Configured</th>
<th>The configured split-mode of the port. (AUTO/4X10G/4X25G/40G/100G)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>The current operational split-mode of the port. (AUTO/4X10G/4X25G/40G//100G/None)</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- interfaces primary-port split-mode: Configures the mode of the splitter cable capable ports.

**MIB Objects**

- esmPortModeTable
  - esmConfiguredMode
show interfaces break-out

Displays the configured and operational state of the 4X10G capable ports.

show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] break-out

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: Display all the ports on the specified slot.
- **port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

By default, information for all ports that support the splitter cable functionality is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The output is only displayed for those ports that support the splitter cable functionality.
- On modules with a single link LED per port, the LED is controlled by the status of sub-port 'A' only.

Examples

`-> show interfaces break-out`

<table>
<thead>
<tr>
<th>Ch/Slot/Port</th>
<th>Split-Mode</th>
<th>Configured</th>
<th>Operational</th>
<th>Member-Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1A</td>
<td>4X10</td>
<td>4X10G</td>
<td>1/1/1A-1/1/1D</td>
<td></td>
</tr>
<tr>
<td>1/1/2A</td>
<td>AUTO</td>
<td>40G</td>
<td>1/1/2A-1/1/2D</td>
<td></td>
</tr>
<tr>
<td>1/1/3A</td>
<td>40G</td>
<td>40G</td>
<td>1/1/3A-1/1/3D</td>
<td></td>
</tr>
<tr>
<td>1/1/4A</td>
<td>AUTO</td>
<td>None</td>
<td>1/1/4A-1/1/4D</td>
<td></td>
</tr>
</tbody>
</table>

<output truncated>

Output definitions

- **Ch/Slot/Port**: The chassis, slot, and port.
output definitions (continued)

<table>
<thead>
<tr>
<th>Configured</th>
<th>The configured split-mode of the port. (AUTO/4X10G/4X25G/40G/100G)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational</td>
<td>The current operational split-mode of the port. (AUTO/4X10G/4X25G/40G//100G/None)</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.7R3; command introduced.

**Related Commands**

`interfaces port break-out` Configures the mode of the splitter cable capable ports.

**MIB Objects**

`esmPortModeTable`  
`esmConfiguredMode`
**show transceivers**

Displays transceiver manufacturer and status information.

`show transceivers [slot chassis/slot [transceiver transceiver_num]]`

**Syntax Definitions**

- **chassis**
  - The chassis identifier.
- **slot**
  - Display all the ports on the specified slot.
- **transceiver_num**
  - The number of the transceiver to display.

**Defaults**

By default, information is displayed for all transceivers.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify a chassis/slot number to display transceiver information for a specific module.
- Specify a transceiver model number to display information for a specific transceiver.

**Examples**

```
-> show transceivers
Chassis ID 1
Slot 1 Transceiver 53
  ALU Model Name:  QSFP-40G-C1M
  ALU Model Number:  120387-90
  Hardware Revision:  A
  Serial Number:  404820066
  Manufacture Date:  Feb 17 2014
  Laser Wave Length:  N/A
  Admin Status:  POWER ON
  Operational Status:  UP

Chassis ID 2
Slot 1 Transceiver 30
  ALU Model Name:  QSFP-40G-C1M
  ALU Model Number:  120387-90
  Hardware Revision:  A
  Serial Number:  404820066
```
Manufacture Date: Feb 17 2014,
Laser Wave Length: N/A,
Admin Status: POWER ON,
Operational Status: UP

Slot 1 Transceiver 39
Manufacturer Name: PICOLIGHT,
Part Number: PL-XPL-00-S13-00,
Hardware Revision: ,
Serial Number: P100Q1F,
Manufacture Date: Jul 2 2002,
Laser Wave Length: N/A,
Admin Status: POWER ON,
Operational Status: UP

-> show transceivers slot 2/1
Slot 1 Transceiver 30
ALU Model Name: QSFP-40G-C1M,
ALU Model Number: 120387-90,
Hardware Revision: A,
Serial Number: 404820066,
Manufacture Date: Feb 17 2014,
Laser Wave Length: N/A,
Admin Status: POWER ON,
Operational Status: UP

Slot 1 Transceiver 39
Manufacturer Name: PICOLIGHT,
Part Number: PL-XPL-00-S13-00,
Hardware Revision: ,
Serial Number: P100Q1F,
Manufacture Date: Jul 2 2002,
Laser Wave Length: N/A,
Admin Status: POWER ON,
Operational Status: UP

-> show transceivers slot 2/1 transceiver 39
Slot 1 Transceiver 39
Manufacturer Name: PICOLIGHT,
Part Number: PL-XPL-00-S13-00,
Hardware Revision: ,
Serial Number: P100Q1F,
Manufacture Date: Jul 2 2002,
Laser Wave Length: N/A,
Admin Status: POWER ON,
Operational Status: UP

output definitions

<table>
<thead>
<tr>
<th>Manufacturer Name</th>
<th>The name of the transceiver’s manufacturer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part Number</td>
<td>The part number of the transceiver.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>The hardware revision of the transceiver.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the transceiver.</td>
</tr>
<tr>
<td>Manufacture Date</td>
<td>The manufacture date of the transceiver.</td>
</tr>
<tr>
<td>Laser Wave Length</td>
<td>The laser wavelength of the transceiver.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Admin Status</th>
<th>The administrative status of the transceiver.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Status</td>
<td>The operational status of the transceiver.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`show interfaces ddm` Displays the DDM administrative status or trap capability.

**MIB Objects**

N/A
show violation

Displays the violation conditions that exist on specific ports or link aggregates.

`show violation [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]`

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number of a specific interface to display. Use a hyphen to specify a range of ports.
- `agg_id[-agg_id2]` Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

NA

**Examples**

In the following example, the `admin down` action for link aggregate 2 indicates that a port violation has occurred on one of the ports related to the link aggregate group with ID 2.

```
-> show violation
* = Link Agg ID
LAG ID/Port  Source  Action       Reason         WTR  Time  Max/Remain
----------+----------+------------------+---------------+-----+---------+----------
1/1/1     src lrn   simulated down  lps shutdown     0    300     10/5
1/1/1     src lrn   simulated down  lps restrict      0    300     10/10
*0/2      qos       admin down     policy          0    300     10/10
```

**output definitions**

- **Port** The slot and port numbers or link aggregate IDs on which violations occurred.
- **Source** Specifies the source application that detected the violation.
**output definitions**

<table>
<thead>
<tr>
<th>Action</th>
<th>Specifies the action that is taken when the violation is detected on the port. There are two types of actions: admin down - deactivates the physical port. simulated down - the port is put in blocking state.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason</td>
<td>Specifies the reason for the violation.</td>
</tr>
<tr>
<td>WTR</td>
<td>The wait-to-restore timer value. Specifies the number of seconds the switch waits before notifying other applications that the link is up. Configured through the interfaces wait-to-restore command.</td>
</tr>
<tr>
<td>Recovery Time</td>
<td>The amount of time after which the port is automatically re-activated if the port was shutdown. Configured through the violation recovery-time command.</td>
</tr>
<tr>
<td>Recovery Max/Remain</td>
<td>The maximum number of recovery attempts allowed and the number of attempts remaining. Configured through the violation recovery-maximum command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

clear violation

Clears all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation.

**MIB Objects**

portViolationTable
  - portViolationSource
  - portViolationEntry
  - portViolationTrap
  - portViolationSource
  - portViolationReason
  - portViolationAction
  - portViolationTimer
  - portViolationTimerAction
**show interfaces portgroup**

Displays the port group mappings on an applicable OmniSwitch.

`show interfaces portgroup [slot chassis/slot | port-group-number chassis/slot/group[-group]]`

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` Slot number to display information about all ports on a specific slot.
- `group[-group]` The group number. Use a hyphen to specify a range of groups.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6900 V48C8 No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The OmniSwitch 6900-V48C8 does not support a mix of 1G/10G and 25G speeds on the 4-port groups of ports 1-48 listed below. Mixing 1G and 10G speeds is supported.
- Member ports of each port group are non-contiguous, use this command to display the port mapping.

---

**Examples**

```
-> show interfaces portgroup
Ch/                                           Ch/
Slot/                   Speed                 Slot
Port-Group-Num   Configured   Operational     Member-Port
--------------+--------------+-------------+---------------
1/1/1                 25G          None        1,2,3,6,
1/1/2                 AUTO         10G         4,5,7,9,
1/1/3                 AUTO         10G         8,10,11,12,
1/1/4                 AUTO         None        13,14,15,18,
1/1/5                 AUTO         None        16,17,19,21,
1/1/6                 AUTO         25G         20,22,23,24,
1/1/7                 AUTO         None        25,26,27,30,
1/1/8                 AUTO         25G         28,29,31,33,
1/1/9                 AUTO         25G         32,34,35,36,
1/1/10                AUTO         None        37,38,39,42,
1/1/11                AUTO         None        40,41,43,45,
```
show interfaces portgroup

1/1/12        AUTO       None     44,46,47,48,

output definitions

Ch/Slot/Port-Group-Num  The port group number (1-12).
Configured Speed       The configured speed of the port group (Auto, 25G, 10G).
Operational            The operational speed of the port group.
Ch/Slot/Member-Port     The member ports of the corresponding port group.

Release History

Release 8.7R2; command introduced.

Related Commands

interfaces portgroup       Configures the speed of the port group.

MIB Objects

esmPortGroupTable
  esmPortGroupEntry
  esmPortGroupIfIndex
  esmConfiguredPortGroupSpeed
  esmOperationalPortGroupSpeed
show violation-recovery-configuration

Displays the global violation recovery configuration details (recovery trap, recovery maximum, and recovery time.

show violation-recovery-configuration {slot chassis/slot | port chassis/slot/port[-port2]}

Syntax Definitions

- `chassis`: The chassis identifier.
- `slot`: The slot number for a specific module.
- `port[-port2]`: The port number. Use a hyphen to specify a range of ports.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show violation-recovery-configuration
Global Violation Trap : enable
Global Recovery Maximum : 20
Global Recovery Time : 200

<table>
<thead>
<tr>
<th>Port</th>
<th>Recovery Max</th>
<th>Recovery Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>10</td>
<td>300</td>
</tr>
<tr>
<td>1/1/2</td>
<td>10</td>
<td>300</td>
</tr>
</tbody>
</table>

-> show violation-recovery-configuration port 3/1/1-2
Global Recovery Trap : enable
Global Recovery Maximum : 20
Global Recovery Time : 200

<table>
<thead>
<tr>
<th>Port</th>
<th>Recovery Max</th>
<th>Recovery Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/1/1</td>
<td>10</td>
<td>300</td>
</tr>
<tr>
<td>3/1/2</td>
<td>10</td>
<td>300</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Output Definitions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Violation Trap</td>
<td>Displays the global status of the violation trap recovery.</td>
</tr>
<tr>
<td>Global Recovery Maximum</td>
<td>Displays the global value set for the maximum violation recovery.</td>
</tr>
<tr>
<td>Global Recovery Time</td>
<td>Displays the global value set for the recovery time.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the chassis, slot and port numbers or link aggregate IDs on which address violations occurred.</td>
</tr>
<tr>
<td>Recovery Max</td>
<td>Displays the maximum number of retry configured.</td>
</tr>
<tr>
<td>Recovery Time</td>
<td>Displays the duration taken for recovery.</td>
</tr>
</tbody>
</table>

Release History

Release 8.2.1; command introduced.

Related Commands

clear violation

Clears all the MAC address violation logs for a particular port and session. After the violations are cleared, the specific port resumes normal operation.

violation recovery-maximum

Configures the maximum number of recovery attempts allowed before the port is permanently shut down.

violation recovery-time

Configures the time interval after which the port is automatically re-activated if the port was shutdown for any violation.

violation recovery-trap

Enables or disables the sending of a violation recovery trap when any port is re-enabled after the violation recovery time has expired.

MIB Objects

portViolationTable

alaPvrGlobalTrapEnable
alaPvrGlobalRetryTime
alaPvrGlobalRecoveryMax
alaPvrRetryTime
alaPvrRecoveryMax
**interfaces link-monitoring admin-status**

Enables or disables link monitoring on a specific slot, port, or a range of specified ports.

`interfaces {slot chassis/slot | port chassis/slot/port[-port2]} link-monitoring admin-status {enable | disable}`

---

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot**
  - The slot number for a specific module.

- **port[-port2]**
  - The port number. Use a hyphen to specify a range of ports.

- **enable**
  - Enables link monitoring for the specified port.

- **disable**
  - Disables link monitoring for the specified port.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Configuring link monitoring parameters are allowed even if the link monitoring status is disabled for the specified ports.

- The Automatic Recovery Timer and link monitoring must not be enabled on Remote Fault Propagation (RFP) enabled ports.

- Enter a slot number to configure link monitoring for all interfaces on a specific slot.

- Enter a slot and port number or a range of port numbers to configure link monitoring for a specific interface or range of interfaces.

- Link Monitoring can be enabled on the member ports of the link aggregate, but not on the entire link aggregate. Link Monitoring is not supported on the VFL ports.

---

**Example**

```
-> interfaces slot 1/1 link-monitoring admin-status enable
-> interfaces port 1/1/1 link-monitoring admin-status enable
```
interfaces port 1/1/1-7 link-monitoring admin-status enable
interfaces port 1/2/5 link-monitoring admin-status disable
interfaces port 1/2/5-20 link-monitoring admin-status disable

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- `show interfaces` Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
- `show interfaces ddm` Displays the link monitoring configuration for the specified ports.
- `show interfaces link-monitoring statistics` Displays the link monitoring statistics for the specified ports.

**MIB Objects**

- `alaLinkMonConfigTable`  
- `alaLinkMonStatus`
interfaces link-monitoring time-window

Configures the monitoring time window on a specific slot, port, or a range of specified ports. This is the length of time during which the link is monitored.

`interfaces {slot chassis/slot | port chassis/slot/port[-port2]} link-monitoring time-window seconds`

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot`: The slot number for a specific module.
- `port[-port2]`: The port number. Use a hyphen to specify a range of ports.
- `seconds`: The length of time during which the link is monitored. The valid range is 0–3600 seconds.

**Defaults**

By default, the time window value is set to 300 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

| 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | V72/C32 | 6900 | X48C6/T48C6/ | 9900 |
|------|------|------|-------|------|-------|------|------|---------|------| X48C4E/V48C8/ |      |
| Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes     | Yes  | C32E/T24C2/ |      |
|      |      |      |       |      |       |      |      |         |      | X24C2      |      |

**Usage Guidelines**

- Enter a slot number to configure the monitoring time window for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the monitoring time window for a specific interface or a range of interfaces.

**Example**

```
-> interfaces slot 1/1 link-monitoring time-window 20
-> interfaces port 1/1/1 link-monitoring time-window 40
-> interfaces port 1/1/1-7 link-monitoring time-window 2500
```

**Release History**

Release 7.3.2; command introduced.
Related Commands

- `show interfaces` Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
- `show interfaces link-monitoring config` Displays the link monitoring configuration for the specified ports.
- `show interfaces link-monitoring statistics` Displays the link monitoring statistics for the specified ports.

MIB Objects

- `alaLinkMonConfigTable`
  - `alaLinkMonTimeWindow`
interfaces link-monitoring link-flap-threshold

Configures the number of link flaps allowed on a specific slot, port, or a range of specified ports in the time interval, before the port is shutdown.

```
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} link-monitoring link-flap-threshold
link_flaps
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.
- `link_flaps` The number of link flaps. The valid range is 2-10.

**Defaults**

By default, the number of link flaps allowed is set to 5.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter a slot number to configure the number of link flaps allowed for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the number of link flaps allowed for a specific interface or a range of interfaces.

**Example**

```
--> interfaces slot 1/1 link-monitoring link-flap-threshold 6
--> interfaces port 1/1/1 link-monitoring link-flap-threshold 3
--> interfaces port 1/1/1-7 link-monitoring link-flap-threshold 10
```

**Release History**

Release 7.3.2; command introduced.
**Related Commands**

*show interfaces*  
Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

*show interfaces ddm*  
Displays the link monitoring configuration for the specified ports.

*show interfaces link-monitoring statistics*  
Displays the link monitoring statistics for the specified ports.

**MIB Objects**

alaLinkMonConfigTable
  - alaLinkMonLinkFlapThreshold
interfaces link-monitoring link-error-threshold

Configures the number of MAC errors allowed on a specific slot, port, or a range of specified ports in the time interval, before the port is shutdown. MAC errors refer to lost frames, error frames, alignment frames and cyclic redundancy check (CRC).

```
interfaces {slot chassis/slot| port chassis/slot/port[-port2]} link-monitoring link-error-threshold
mac_errors
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.
- **mac_errors**: The number of MAC errors. The valid range is 1-100.

**Defaults**

By default, the number of MAC errors allowed is set to 5.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter a slot number to configure the number of MAC errors allowed on all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to configure the number of MAC errors allowed on a specific interface or on a range of interfaces.

**Example**

```
-> interfaces slot 1/1 link-monitoring link-error-threshold 30
-> interfaces port 1/1/1 link-monitoring link-error-threshold 10
-> interfaces port 1/1/1-7 link-monitoring link-error-threshold 35
```

**Release History**

Release 7.3.2; command introduced.
**Related Commands**

- **show interfaces**
  Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

- **show interfaces ddm**
  Displays the link monitoring configuration for the specified ports.

- **show interfaces link-monitoring statistics**
  Displays the link monitoring statistics for the specified ports.

**MIB Objects**

- `alaLinkMonConfigTable`
  - `alaLinkMonLinkErrorThreshold`
interfaces clear-link-monitoring-stats

Clears the link monitoring statistics on a specific slot, port, or a range of specified ports.

```
interfaces {slot chassis/slot| port chassis/slot/port[-port2]} clear-link-monitoring-stats
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a slot number to clear monitoring statistics for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to clear monitoring statistics for a specific interface or a range of interfaces.

### Example

- `-> interfaces slot 1/1 clear-link-monitoring-stats`
- `-> interfaces port 1/1/1 clear-link-monitoring-stats`
- `-> interfaces port 1/1/1-7 clear-link-monitoring-stats`

### Release History

Release 7.3.2; command introduced.
Related Commands

- **show interfaces**
  Displays the administrative, operational, violation, and recovery status and configuration for the specified port.

- **show interfaces ddm**
  Displays the link monitoring configuration for the specified ports.

- **show interfaces link-monitoring statistics**
  Displays the link monitoring statistics for the specified ports.

MIB Objects

- **alaLinkMonStatsTable**
  - **alaLinkMonStatsClearStats**
show interfaces link-monitoring config

Displays configuration information for the Link Monitoring feature. This includes the link monitoring status on a specific slot, port or a range of specified ports, time window, link flap threshold, and link error threshold.

**show interfaces {slot chassis/slot| port chassis/slot/port|-port2]} link-monitoring config**

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot**
  - The slot number for a specific module.

- **port[-port2]**
  - The port number. Use a hyphen to specify a range of ports.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

### Example

```bash
-> show interfaces slot 1/1 link-monitoring config
Ch/Slot/ Status   Time   Link-flap Threshold  Link-error Threshold
Port   Window (sec)
      -------------------------+-------------------------+
1/1/1   enabled 10     5          10         
1/1/2   disabled 10     5          10         
1/1/3   disabled 200    8          20         
.        .          .          .           
1/1/24  disabled 150    2          99         
```
show interfaces port 1/1/1-3 link-monitoring config

<table>
<thead>
<tr>
<th>Slot/ Port</th>
<th>Status</th>
<th>Time Window</th>
<th>Link-flap Threshold</th>
<th>Link-error Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>enabled</td>
<td>10</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>1/1/2</td>
<td>disabled</td>
<td>10</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>1/1/3</td>
<td>disabled</td>
<td>200</td>
<td>7</td>
<td>99</td>
</tr>
</tbody>
</table>

show interfaces port 1/1/1 link-monitoring config

<table>
<thead>
<tr>
<th>Slot/ Port</th>
<th>Status</th>
<th>Time Window</th>
<th>Link-flap Threshold</th>
<th>Link-error Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>enabled</td>
<td>10</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

show interfaces port 1/1/2 link-monitoring config

<table>
<thead>
<tr>
<th>Slot/ Port</th>
<th>Status</th>
<th>Time Window</th>
<th>Link-flap Threshold</th>
<th>Link-error Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>disabled</td>
<td>10</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

output definitions

- **Ch/Slot/Port**: Interface chassis, slot, and port number.
- **Status**: Link monitoring status (enable/disable).
- **Time Window**: Time interval, in seconds, for which the link is monitored.
- **Link-flap threshold**: Number of link flaps allowed on a specific slot, port, or a range of specified ports in the time interval before the port is shutdown.
- **Link-error threshold**: Number of MAC errors allowed on a specific slot, port, or a range of specified ports in the time interval before the port is shutdown.

Release History

Release 7.3.2; command introduced.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces</code></td>
<td>Displays information of the interface port status.</td>
</tr>
<tr>
<td><code>show interfaces link-monitoring statistics</code></td>
<td>Displays the Link Monitoring statistics.</td>
</tr>
<tr>
<td><code>interfaces link-monitoring admin-status</code></td>
<td>Enables or disables link monitoring.</td>
</tr>
<tr>
<td><code>interfaces link-monitoring time-window</code></td>
<td>Configures the monitoring of the time-window of the link.</td>
</tr>
<tr>
<td><code>interfaces link-monitoring link-flap-threshold</code></td>
<td>Configures the number of link flaps that are allowed before the port is shutdown.</td>
</tr>
<tr>
<td><code>interfaces link-monitoring link-error-threshold</code></td>
<td>Configures the number of MAC errors that are allowed before the port is shutdown.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- `alaLinkMonConfigTable`
  - `alaLinkMonStatus`
  - `alaLinkMonTimeWindow`
  - `alaLinkMonLinkFlapThreshold`
  - `alaLinkMonLinkErrorThreshold`
show interfaces link-monitoring statistics

Displays the Link Monitoring statistics for a specific slot, port, or a range of specified ports.

`show interfaces {slot chassis/slot| port chassis/slot/port[-port2]} link-monitoring statistics`

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port[-port2]` The port number. Use a hyphen to specify a range of ports.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter a slot number to display information for all interfaces on a specific port.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or a range of interfaces.

**Example**

```
-> show interfaces slot 1/1 link-monitoring statistics
Ch/ Slot/ State Current Current Current Current Current Current Total Total
 Port Flap Error CRC Lost Align Flap Error
-----------------------------------------------
1/1/1 shutdown 6 3 2 0 0 15 6
1/1/2 down 3 2 1 0 0 12 3
.
1/1/24 up 3 2 1 0 0 12 3

-> show interfaces port 1/1/1-2 link-monitoring statistics
Ch/ Slot/ State Current Current Current Current Current Current Total Total
 Port Flap Error CRC Lost Align Flap Error
-----------------------------------------------
1/1/1 shutdown 6 3 2 0 0 15 6
```
1/1/2   down        3       2         1         0         0       12      3

-> show interfaces port 1/1/1 link-monitoring statistics

<table>
<thead>
<tr>
<th>Ch/</th>
<th>Slot/</th>
<th>State</th>
<th>Current Flap</th>
<th>Current Error</th>
<th>Current CRC</th>
<th>Current Lost</th>
<th>Current Align</th>
<th>Current Flap</th>
<th>Current Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>1/1</td>
<td>shutdown</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>6</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- `show interfaces` Displays the administrative, operational, violation, and recovery status and configuration for the specified port.
- `show interfaces link-monitoring config` Displays configuration information of the Link Monitoring.
- `interfaces link-monitoring admin-status` Enables or disables link monitoring.
- `interfaces clear-link-monitoring-stats` Clears the Link Monitoring statistics.
- `interfaces link-monitoring link-error-threshold` Configures the number of MAC errors that are allowed before the port is shutdown.

**MIB Objects**

- `alaLinkMonStatsTable`
  - `alaLinkMonStatsPortStatus`
  - `alaLinkMonStatsCurrentLinkFlaps`
  - `alaLinkMonStatsCurrentErrorFrames`
  - `alaLinkMonStatsCurrentCRCErrors`
  - `alaLinkMonStatsCurrentLostFrames`
  - `alaLinkMonStatsCurrentAlignErrors`
  - `alaLinkMonStatsCurrentLinkErrors`
  - `alaLinkMonStatsTotalLinkFlaps`
  - `alaLinkMonStatsTotalLinkErrors`
**interfaces tdr**

Initiates a Time Domain Reflectometry (TDR) cable diagnostics test on the specified port. The TDR feature sends a signal down a cable to determine the distance to a break or other discontinuity in the cable path. The length of time it takes for the signal to reach the break and return is used to estimate the distance to the discontinuity.

**interfaces port chassis/slot/port tdr enable**

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `port` The port number.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- TDR is an on-demand, out-of-service test. The test is not automatically triggered; data and protocol traffic is interrupted.
- Only one TDR test can be run at any given time.
- TDR is not supported on link aggregate ports, fiber ports, or stacking ports.
- TDR results are automatically cleared when a new test is started on the port or when the module for the port is reset.

---

**Examples**

- `-> interfaces port 1/1/1 tdr enable`

---

**Release History**

Release 8.1.1; command was introduced.
Related Commands

- **clear interfaces**: Clears the statistics of the last test performed on the port.
- **show interfaces tdr-statistics**: Displays the results of the last TDR test performed on a port.

MIB Objects

- esmTdrPortTable
- esmTdrPortTest
show interfaces tdr-statistics

Displays the results of the last TDR test performed on a port.

**show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] tdr-statistics**

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: The slot number for a specific module.
- **port[-port2]**: The port number. Use a hyphen to specify a range of ports.

**Defaults**

By default, TDR statistics are shown for all ports on all modules

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter a slot number to display information for all interfaces on a specific slot.
- Enter a slot and port number or a range of port numbers to display information for a specific interface or range of interfaces.

**Examples**

```bash
-> show interfaces port 1/1/3 tdr-statistics
Ch/Slot/Port       No of Fuzzy Pair1 Pair1 Pair2 Pair2 Pair3 Pair3 Pair4 Pair4 Test
-----------------+-------+-------+-------+-------+-------+-------+-------+-------+----------------
Port Pairs Len   State Len State Len State Len State Len State Len Results-----------------+-------+-------+-------+-------+-------+-------+-------+-------+----------------
1/1/1 4 10       Open  0     Open  0     Open  0     Open  0     Open  0     Success
```

**output definitions**

- **Ch/Slot/Port**: The interface chassis, slot, and port number.
- **No of pairs**: The number of pairs in the cable for which the test results are valid.
- **Fuzzy Length**: The error in the estimated length of the cable.
output definitions (continued)

<table>
<thead>
<tr>
<th>Cable State</th>
<th>State of a cable as returned by the TDR test. The state of the cable wire.</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) OK</td>
<td>Wire is working properly</td>
</tr>
<tr>
<td>(b) Open</td>
<td>Wire is broken</td>
</tr>
<tr>
<td>(c) Short</td>
<td>Pairs of wire are in contact with each other</td>
</tr>
<tr>
<td>(d) Crosstalk</td>
<td>Signal transmitted on one pair of wire creates an undesired effect in another wire.</td>
</tr>
<tr>
<td>(e) Unknown</td>
<td>Cable diagnostic test unable to find the state of a cable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pair1 State</th>
<th>The state of the Pair 1 cable wire (OK, Open, Short, Crosstalk, or Unknown)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pair1 Length</td>
<td>The length of the Pair 1 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pair2 State</th>
<th>The state of the Pair 2 cable wire (OK, Open, Short, Crosstalk, or Unknown)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pair2 Length</td>
<td>The length of the Pair 2 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pair3 State</th>
<th>The state of the Pair 3 cable wire (OK, Open, Short, Crosstalk, or Unknown)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pair3 Length</td>
<td>The length of the Pair 3 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Pair4 State</th>
<th>The state of the Pair 4 cable wire (OK, Open, Short, Crosstalk, or Unknown)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pair4 Length</td>
<td>The length of the Pair 4 cable at which the fault is detected, if the pair is faulty. Else, specifies the complete length of the cable.</td>
</tr>
</tbody>
</table>

| Test Result   | The status of the TDR test performed, success or fail. |

Release History

Release 8.1.1 command was introduced.

Related Commands

<table>
<thead>
<tr>
<th>interfaces tdr</th>
<th>Initiates the cable diagnostics on a port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear interfaces</td>
<td>Clears the statistics of the last test performed on the port.</td>
</tr>
</tbody>
</table>

MIB Objects

esmTdrPortTable

  esmTdrPortCableState
  esmTdrPortValidPairs
  esmTdrPortPair1State
  esmTdrPortPair1Length
  esmTdrPortPair2State
  esmTdrPortPair2Length
  esmTdrPortPair3State
  esmTdrPortPair3Length
  esmTdrPortPair4State
  esmTdrPortPair4Length
  esmTdrPortFuzzLength
**link-fault-propagation group**

Configures a Link Fault Propagation (LFP) group to associate with source and destination ports.

```bash
link-fault-propagation group group_id [admin-status {enable | disable}]
no link-fault-propagation group {group_id[-group_id2]}
```

**Syntax Definitions**

- `group_id`  
  A group ID number. The valid range is 1–8.

- `group_id[-group_id2]`  
  A group ID number to remove. Use a hyphen to specify a range of existing group ID numbers (5-8). Specifying a range is only used to remove group IDs, not to create them.

- `enable`  
  Enables LFP for the specified group.

- `disable`  
  Disables LFP for the specified group.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a LFP group or a range of groups.
- Up to eight LFP groups per switch are allowed.
- Once a LFP group is created, assign source and destination ports to that group.

**Example**

```bash
-> link-fault-propagation group 1
-> no link-fault-propagation group 4
-> no link-fault-propagation group 4-7
```

**Release History**

Release 7.3.2; command introduced.
Related Commands

- **link-fault-propagation group source**
  Configures the source port assignments for the LFP group.

- **link-fault-propagation group destination**
  Configures the destination port assignments for the LFP group.

- **link-fault-propagation group wait-to-shutdown**
  Configures the amount of time LFP waits before shutting down the destination ports.

- **show link-fault-propagation group**
  Displays the LFP group configuration for the switch.

MIB Objects

- **alaLFPGroupTable**
  - **alaLFPGroupId**
  - **alaLFPGroupRowStatus**
link-fault-propagation group source

Configures the source port assignments for a Link Fault Propagation (LFP) group.

```
link-fault-propagation group group_id source {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

```
no link-fault-propagation group group_id source {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- `group_id`: An existing LFP group ID number. The valid range is 1–8.
- `chassis`: The chassis identifier.
- `slot`: The slot number for a specific module.
- `port[-port2]`: The port number. Use a hyphen to specify a range of ports and/or a space to specify multiple port entries.
- `agg_id[-agg_id2]`: The link aggregate ID number. Use a hyphen to specify a range of IDs and/or a space to specify multiple ID entries (1-5 10 12).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a source port association with the specified LFP group.
- Make sure the LFP group specified with this command already exists in the switch configuration.
- Configuring the source ports and destinations ports for the specified LFP group is allowed within the same command (see the examples on this command page).
- A group can have a maximum of 64 source ports and 64 destination ports.
- A maximum of 64 link aggregates is supported, regardless of the number of ports in each aggregate in a group.
- A port/linkagg added as a source/destination port for a particular group cannot be added as a destination/source port for this group or for any other group.
• If a port is recovered due to the Interface Recovery Timer, then the port will revert to the shutdown state if the error persists.

Example

- `link-fault-propagation group 1 source port 1/2`
- `link-fault-propagation group 1 source port 1/2-5 2/3`
- `link-fault-propagation group 1 source linkagg 1`
- `link-fault-propagation group 1 source linkagg 1-3`
- `link-fault-propagation group 1 source port 2/3 destination port 1/6`
- `link-fault-propagation group 1 source port 3/1-5 destination linkagg 6`
- `no link-fault-propagation group 1 destination port 1/10`

Release History

Release 7.3.2; command introduced.

Related Commands

- `link-fault-propagation group` Configures an LFP group, including the administrative status.
- `link-fault-propagation group destination` Configures the destination port assignments for the LFP group.
- `link-fault-propagation group wait-to-shutdown` Configures the amount of time LFP waits before shutting down the destination ports.
- `show link-fault-propagation group` Displays the LFP group configuration for the switch.

MIB Objects

- `alaLFPGroupTable` (alaLFPGroupId, alaLFPConfigTable) Configures an LFP group, including the administrative status.
- `alaLFPConfigTable` (alaLFPConfigPort, alaLFPConfigPortType, alaLFPConfigRowStatus) Configures the destination port assignments for the LFP group.
**link-fault-propagation group destination**

Configures the destination port assignments for a Link Fault Propagation (LFP) group.

```
link-fault-propagation group group_id destination {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

```
no link-fault-propagation group group_id destination {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- **group_id**
  - An existing LFP group ID number. The valid range is 1–8.
- **chassis**
  - The chassis identifier.
- **port[-port2]**
  - The port number. Use a hyphen to specify a range of ports and/or a space to specify multiple port entries.
- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs and/or a space to specify multiple ID entries (1-5 10 12).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/</th>
<th>6900X48C8/E48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a destination port association with the specified LFP group.
- Make sure the LFP group specified with this command already exists in the switch configuration.
- Configuring the source ports and destinations ports for the specified LFP group is allowed within the same command (see the examples on this command page).
- A group can have a maximum of 64 source ports and 64 destination ports.
- A maximum of 64 link aggregates is supported regardless of the number of ports in each aggregate in a group.
- A port or link aggregate that is configured as a source port cannot be configured as a destination port for any group. However, a source port can be associated with multiple LFP groups.
• A port or link aggregate that is configured as a destination port cannot be configured as a source port for any group. However, a destination port can be associated with multiple LFP groups.

• If port is recovered due to the Interface Recovery Timer, then the port will revert to the shutdown state if the error persists.

Example

-> link-fault-propagation group 1 destination port 1/4
-> link-fault-propagation group 1 destination port 1/5-8 2/3
-> link-fault-propagation group 1 destination linkagg 6
-> link-fault-propagation group 1 destination linkagg 6-10
-> link-fault-propagation group 1 source port 1/2 2/3 destination port 1/6
-> link-fault-propagation group 1 source port 1/2 2/3 destination linkagg 6
-> link-fault-propagation group 1 source linkagg 3 destination port 1/6 1/9
-> link-fault-propagation group 1 source linkagg 3 destination linkagg 1

-> no link-fault-propagation group 1 source port 1/9
-> no link-fault-propagation group 1 destination port 1/10

Release History

Release 7.3.2; command introduced.

Related Commands

- link-fault-propagation group
  Configures an LFP group, including the administrative status.
- link-fault-propagation group source
  Configures the source port assignments for the LFP group.
- link-fault-propagation group wait-to-shutdown
  Configures the amount of time LFP waits before shutting down the destination ports.
- show link-fault-propagation group
  Displays the LFP group configuration for the switch.

MIB Objects

- alaLFPGroupTable
- alaLFPGroupId
- alaLFPConfigTable
- alaLFPConfigPort
- alaLFPConfigPortType
- alaLFPConfigRowStatus
link-fault-propagation group wait-to-shutdown

Configures the wait-to-shutdown timer value for the Link Fault Propagation (LFP) group. This is the amount of time after all the source ports go down that LFP waits before shutting down the destination ports.

link-fault-propagation group group_id wait-to-shutdown seconds

Syntax Definitions

group_id
An existing LFP group ID number. The valid range is 1–8.

seconds
The number of seconds LFP waits before shutting down the destination ports. The valid range is 0-300 in multiples of 5.

Defaults

By default, the timer is set to zero (disabled).

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Set the wait-to-shutdown timer value to 0 to disable the timer.
- Make sure the LFP group specified with this command already exists in the switch configuration.

Example

-> link-fault-propagation group 1 wait-to-shutdown 40
-> link-fault-propagation group 3 wait-to-shutdown 70
-> link-fault-propagation group 5 wait-to-shutdown 0

Release History

Release 7.3.2; command introduced.
Related Commands

- link-fault-propagation group
  - Configures an LFP group, including the administrative status.
- show link-fault-propagation group
  - Displays the LFP group configuration for the switch.

MIB Objects

alaLFPGroupTable
  - alaLFPGroupId
  - alaLFPGroupWaitToShutdown
  - alaLFPGroupRowStatus
show link-fault-propagation group

 Displays information for the specified Link Fault Propagation (LFP) group.

 show link-fault-propagation group [group_id]

**Syntax Definitions**

`group_id` An existing LFP group ID number. The valid range is 1–8.

**Defaults**

By default, information is displayed for all existing LFP groups.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter a LFP group ID number with this command to display information for a specific group.
- If a virtual port such as a link aggregate is configured as a source or destination port it will be displayed instead of the physical ports.

**Example**

```bash
-> show link-fault-propagation group
Group Id : 2
    Source Port(s) : 0/1-2 1/1/1-5 1/1/7,
    Destination Port(s) : 0/3 1/1/10-13,
    Group-Src-Ports Status : up,
    Admin Status : enable,
    Wait To Shutdown : 10

Group Id : 7
    Source Port(s) : 1/1/1 1/1/3,
    Destination Port(s) : 0/3 1/1/5 1/1/7 1/1/11 1/1/13 1/1/15 1/1/17 1/1/19 1/1/21 1/1/23,
    Group-Src-Ports Status : up,
    Admin Status : enable,
    Wait To Shutdown : 100
```
-> show link-fault-propagation group 2
  Group Id : 2
  Source Port(s) : 0/1-2 1/1/1-5 1/1/7,
  Destination Port(s) : 0/3 1/1/10-13,
  Group-Src-Ports Status : up,
  Admin Status : enable,
  Wait To Shutdown : 10

Release History
Release 7.3.2; command introduced.

Related Commands
link-fault-propagation group Configures a LFP group, including the administrative status.
link-fault-propagation group wait-to-shutdown Configures the amount of time LFP waits before shutting down the destination ports.

MIB Objects
alaLFPConfTable
  alaLFPConfPort
  alaLFPConfPortType
alaLFPGroupTable
  alaLFPGroupId
    alaLFPGroupAdminStatus
    alaLFPGroupOperStatus
    alaLFPGroupWaitToShutdown
**interfaces beacon**

Configures the LED color and behavior for a port or group of ports.

```
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} beacon [admin-status {enable | disable}] [led-color color] [led-mode {solid | activity}]
```

```
no interfaces {slot chassis/slot | port chassis/slot/port[-port2]} beacon
```

**Syntax Definitions**

- **chassis**: The chassis ID for the switch on which the LEDs are being configured. For standalone switches, use 1.
- **slot**: The slot ID for the switch on which the LEDs are being configured. For standalone switches, use 1.
- **port**: The port number of the interface LED you want to configure.
- **-port2**: The last port number in a range of interface LEDs you want to configure. Be sure to insert a hyphen between port range numbers (for example, 7-10)
- **led-mode**: Indicates that LED behavior (activity or solid) is being configured for the corresponding interface LEDs.
- **activity**: The LEDs will blink when traffic is detected on the corresponding ports.
- **solid**: The LEDs will remain solid whether or not traffic is detected on the corresponding ports.
- **led-color**: Indicates that the LED color is being configured for the corresponding port(s).
- **color**: The color to be displayed on the corresponding port LED(s). Options include yellow, white, red, magenta, green, blue, aqua and off.
- **admin-status**: Indicates that the beacon LED administrative status is being configured for the corresponding port(s).
- **enable**: Enables the beacon function on the corresponding port(s).
- **disable**: Disables the beacon function on the corresponding port(s).
- **no**: Adding the no syntax to the beginning of the command clears all information stored in the beacon settings table. Refer to Usage Guidelines below for more information.
Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>led-mode</td>
<td>activity</td>
</tr>
<tr>
<td>led-color</td>
<td>magenta</td>
</tr>
<tr>
<td>admin-status</td>
<td>enable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Supported on the OmniSwitch 6900-X72/Q32 models only.
- The `no interfaces beacon` command syntax clears the beacon settings from the `show interfaces beacon` table and resets LEDs to original factory-set behavior. (Once stored beacon settings are cleared, they can no longer be retrieved and beacon settings must be reconfigured.)
- The `interfaces beacon` command is supported on all Ethernet ports on the switch. However, when specifying a range in the command line, please note that The Beacon LED feature is not supported on sub-ports 'b', 'c', or 'd' when an interface is operating in 4X10G mode. Additionally, only Solid mode is supported on sub-port 'a' for 4X10G interfaces.

Examples

- `interfaces port 1/1/7-10 beacon led-mode solid admin-status enable led-color aqua`
- `interfaces slot 1/1 beacon led-color magenta`
- `no interfaces slot 1/1/1 beacon`

Release History

Release 7.3.4; command introduced.

Related Commands

- `show interfaces beacon` Displays current interface beacon settings.

MIB Objects

- `esmPortBeaconTable`
- `esmPortBeaconEntry`
- `esmBeaconAdminState`
- `esmBeaconLedColor`
- `esmBeaconLedMode`
show interfaces beacon

Displays current interface beacon settings.

```plaintext
show interfaces [slot chassis/slot | port chassis/slot/port[-port2]] beacon
```

**Syntax Definitions**

- `chassis` The chassis ID for the switch on which beacon settings are being shown. For standalone switches, use 1.
- `slot` The slot ID for the switch on which beacon settings are being shown. For standalone switches, use 1.
- `port` The port number for which beacon settings are being shown.
- `-port2` The last port number in a range for which beacon settings are being shown. Be sure to insert a hyphen between port range numbers (for example, 7-10)

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Supported on the OmniSwitch 6900-X72/Q32 models only.

**Examples**

```plaintext
-> show interfaces beacon
Ch/Slot/Port   Admin-Stat   LED-Color  LED-Mode
------------+-------------+--------------+------------
1/1/1A        Disable     Magenta    Solid
1/1/2A        Disable     Blue       Activity
1/1/30A       Enable      Magenta    Solid
1/1/31A       Enable      Off        Solid
```

**output definitions**

- **Ch/Slot/Port** The chassis/slot/port ID for the switch on which beacon settings are being shown.
- **Admin-Stat** The beacon administrative status (Enable/Disable).
output definitions (continued)

<table>
<thead>
<tr>
<th>LED-Color</th>
<th>The LED color being displayed on the corresponding interface LED. Options include yellow, white, red, magenta, green, blue, aqua and off.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED-Mode</td>
<td>The current LED behavior on the corresponding interface LED. Options include solid or activity (default).</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command introduced.

Related Commands

 interfaces beacon Allows network administrators to change LED color and behavior from a remote location.

MIB Objects

esmPortBeaconTable
  esmPortBeaconEntry
  esmBeaconAdminState
  esmBeaconLedColor
  esmBeaconLedMode
  esmBeaconRowStatus
interfaces ptp admin-state

Enables or disables IEEE 1588 Precision Time Protocol (PTP) on all the interfaces.

`interfaces ptp admin-state {enable | disable} [loopback-portlist chassis/slot/port chassis/slot/port] [chassis/slot/port] [priority {num | default}]`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enables the PTP end-to-end transparent clock on all the interfaces.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables the PTP end-to-end transparent clock on all the interfaces.</td>
</tr>
<tr>
<td><code>chassis</code></td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td><code>slot/port</code></td>
<td>The slot and port number (for example, 3/1).</td>
</tr>
<tr>
<td><code>num</code></td>
<td>Set the internal priority for the incoming PTP packet. Valid range is 1–7.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Sets the internal priority to the default value 5.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command enables PTP end-to-end transparent clock across all ports.
- PTP end-to-end transparent clock is supported in a standalone mode (virtual chassis of one) and virtual chassis of two. PTP end-to-end on a virtual chassis of two is supported only on OmniSwitch 6900-X72.
- Single loopback port per chassis is required to support PTP in a virtual chassis of two.
- Loopback ports dedicated for PTP must not be used by any other feature. Ensure PTP is configured on unused ports.
- PTP on a virtual chassis of two is not supported on chassis ID 1.
- IGMP snooping must not be configured on PTP reserved IPv4 and IPv6 multicast addresses.
- The two 10G ports, 1/1/27 and 1/1/28 on OmniSwitch 6465-P28 does not support PTP.
- Supported on certain OS6560 models and ports with appropriate FPGA. See the 8.7R2 release notes.
**Examples**

-> interfaces ptp admin-state enable  
-> interfaces ptp admin-state disable  
-> interfaces ptp admin-state enable priority 4  
-> interfaces ptp admin-state enable priority default  
-> interfaces ptp admin-state enable loopback-portlist 2/1/12 3/1/23  
WARNING: User ports 2/1/12 and 3/1/23 will be out of service for users.

**Release History**

Release 8.4.1 R02; command introduced.  
Release 8.4.1 R03; OmniSwitch 6860, 6865 support for PTP added.  
Release 8.5R1; OmniSwitch 6465 support for PTP added.  
Release 8.5R2; **loopback-portlist** keyword added.

**Related Commands**

*show interfaces ptp config* Displays the current IEEE 1588 Precision Time Protocol (PTP) status on the switch.

**MIB Objects**

alaPtpConfiguration  
allaPtpConfigAdminStatus  
allaPtpConfigPriority  
allaPtpConfigMode  
allaPtpLoopBackPort1  
allaPtpLoopBackPort2  
allaPtpLoopBackPort3  
allaPtpLoopBackPort4  
allaPtpLoopBackPort5  
allaPtpLoopBackPort6  
allaPtpLoopBackPort7  
allaPtpLoopBackPort8
**interfaces port ptp p2p**

Enables or disables IEEE 1588 PTP peer-to-peer transparent clock on an interface.

```
interfaces port chassis/slot/port ptp p2p admin-state {enable | disable}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (for example, 3/1).
- **enable**: Enables the PTP peer-to-peer transparent clock on an interface.
- **disable**: Disables the PTP peer-to-peer transparent clock on an interface.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- PTP must be enabled globally for PTP peer-to-peer support.
- PTP peer-to-peer supports only one-step mode.
- When peer-to-peer is enabled on a port, link delay will be computed dynamically for the corresponding link.
- Ensure Loopback0 IP interface is configured on the switch as loopback0 interface address will be used as the source IP for peer delay measurement packets. If loopback0 IP interface is not configured, then peer delay measurement feature will not work.

### Examples

```
-> interfaces port 1/1/1 ptp p2p admin-state enable
-> interfaces port 1/1/1 ptp p2p admin-state disable
```

### Release History

Release 8.6R1; command introduced.


**Related Commands**

- **interfaces ptp admin-state**
  Enables or disables IEEE 1588 Precision Time Protocol (PTP) end-to-end transparent clock on the switch.

- **show interfaces ptp config**
  Displays the current IEEE 1588 Precision Time Protocol (PTP) status on the switch.

**MIB Objects**

- a1aPtpPortAdminStatus
- a1aIpServiceSourceIpAppIndex
**show interfaces ptp config**

Displays the current PTP status on the switch.

```
show interfaces ptp config
```

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Peer-to-Peer transparent clock is supported only on the OmniSwitch 6560.

**Examples**

```
-> show interfaces ptp config
```

End-to-End TC:

```
---------------------
Admin-state          : Enabled
Priority              : 5
Chassis-connected     : 2
LoopBack-PortList     : 2/1/12, 3/1/23
```

Peer-to-Peer TC:

```
---------------------
Pkt source-ip    : 1.1.1.1
Port Admin State : 1/1/5
```

---

**output definitions**

**End-to-End TC:**

- **Admin State**
  - The PTP end-to-end administrative status on the switch (Enable/Disable).

- **Priority**
  - The internal priority configured for the incoming PTP packet.
output definitions (continued)

<table>
<thead>
<tr>
<th>Chassis-connected</th>
<th>Number of chassis connected in a virtual chassis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoopBack-PortList</td>
<td>Configured loopback ports to support PTP end-to-end on a virtual chassis of two.</td>
</tr>
<tr>
<td>Peer-to-Peer TC:</td>
<td></td>
</tr>
<tr>
<td>Pkt source-ip</td>
<td>Loopback0 IP interface used as the source IP for peer delay measurement packets.</td>
</tr>
<tr>
<td>Port</td>
<td>The chassis, slot, and port number.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The PTP peer-to-peer administrative status on the switch (Enable/Disable).</td>
</tr>
</tbody>
</table>

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; OmniSwitch 6860, 6865 support for PTP added.
Release 8.5R1; OmniSwitch 6465 support for PTP added.
Release 8.5R2; End-to-End and Peer-to-Peer transparent clock fields added.

Related Commands

- **interfaces ptp admin-state** Enables or disables IEEE 1588 Precision Time Protocol (PTP) end-to-end transparent clock on the switch.
- **interfaces port ptp p2p** Enables or disables IEEE 1588 PTP peer-to-peer transparent clock on an interface.

MIB Objects

N/A
**interfaces macsec admin-state**

This command enables or disables MACsec on a physical port or a port range.

```
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} macsec admin-state {enable | disable}
[transmit-interval tx_interval] [encryption]]
```

```
no interfaces {slot chassis/slot | port chassis/slot/port[-port2]} macsec [sci-rx [hex-num] | sci-tx [keychain [encryption]]]
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot**
  - The slot number for a specific module.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-10).

- **admin-state enable**
  - Enables MACsec on a physical port or port range.

- **admin-state disable**
  - Disables MACsec on a physical port or port range.

- **static**
  - Sets the SA (secure association) mode to static. This is enabled by default.

- **dynamic**
  - Sets the SA (secure association) mode to dynamic.

- **hex-num**
  - The SCI (Secure Channel Identifier) value (up to 8 bytes in length) for Tx and Rx channel in the hexadecimal format (0xhex).
  - The default SCI value is ‘0’ (implicit SCI value).

- **keychain_id**
  - The keychain ID associated to Tx/Rx channel.

- **encryption**
  - Enable or disable the encryption option on the Tx/Rx channel.
  - By default, the ‘encryption’ is disabled.

- **cak_kc**
  - The keychain ID for Static-CAK (Connectivity Association Key).

- **priority**
  - Specifies the server priority in the range 0 to 255.

- **tx_interval**
  - Specifies the transmit interval for MKPDU in the range 2 to 10 seconds.
## Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>priority</td>
<td>5, 10, 15, and 15 respectively on OmniSwitch 9900, OmniSwitch 6860 and OmniSwitch 6860N, OmniSwitch 6465, and OmniSwitch 6560. <strong>Note:</strong> Lower the priority value, higher the precedence.</td>
</tr>
<tr>
<td>tx_interval</td>
<td>2 seconds</td>
</tr>
<tr>
<td>encryption</td>
<td>disabled</td>
</tr>
</tbody>
</table>

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C4E</td>
<td>No</td>
</tr>
</tbody>
</table>

## Usage Guidelines

- Use this command to,
  - Enable or disable MACsec on a physical port or port range.
  - Set the MACsec mode: Static SA Mode or Dynamic SA Mode.

- Only users with MACsec read-write privilege can configure MACsec. Use `user` command to enable MACsec read-write permissions to the users. The privilege can be configured by family or by security domain. For example,
  - `-> user securityadmin password Switch@123 read-write macsec`
  - `-> user securityadmin password Switch@123 read-write domain-security`

  See the “AAA Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide* for more information.

- For Static SA Mode - MACsec with Static Secure Association Key (static-SAK), following configurations can be configured:
  - Set the MACsec mode to Static.
  - Create MACsec Tx and Rx channels.
  - Specify the SCI value for Tx and Rx channels.
  - Associate the keychain ID for Tx and Rx channel. For more information on keychain configuration, refer to the “Chassis Management and Monitoring Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.
  - Enable or disable encryption on Tx and Rx channel (optional).
• Dynamic SA Mode has two variations - Dynamic SAK using pre-shared keys and Dynamic SAK using Extensible Authentication Protocol (EAP).
  – For Dynamic SAK using pre-shared keys, following configurations can be configured:
    > Set the MACsec mode to Dynamic.
    > Configure the keychain for Static-CAK. For more information on keychain configuration, refer to the “Chassis Management and Monitoring Commands” chapter in the OmniSwitch AOS Release 8 CLI Reference Guide.
    > Configure key server priority (optional).
    > Configure transmit interval for MKPDUs (optional).
    > Enable or disable encryption on dynamic secure channel (optional).
  – For Dynamic SAK using EAPs, the following configurations can be configured:
    > Set the MACsec mode to Radius.
    > Configure transmit interval for MKPDUs (optional).
    > Enable or disable encryption on dynamic secure channel (optional).

• By default, the MACsec mode is set to ‘static’. For static mode configuration, manually configured SA keys are used to secure traffic on the point-to-point link between two nodes. For MACsec mode ‘static’, following are the configuration guidelines:
  – Only one Tx and one Rx channel can be configured per interface.
  – Each node that expects to receive traffic sent in a particular transmit secure channel must configure a ‘matching’ receive secure channel, with an SCI corresponding to the SCI of the transmit secure channel of the peer. MACsec supports one secure channel for Tx and one secure channel for Rx configuration on an interface.
  – The secure channel for both Tx and Rx on an interface can be configured with SCI value of 8 bytes long. It can be provided in short form (that is, 0x01) or full form (0x0000000000000001). 0x00 (all zeros) and 0xFFFFFFFFFFFFFFFF SCI value are not valid.
  – The secure channel for both Tx and Rx on an interface can be configured without specifying a SCI value. In this case, the default value will be considered.
  – The keychain associated with the SCI-Tx and SCI-Rx must have four keys supporting ‘AES-GCM-128’ algorithm, and the number of keys in the keychain associated with both SCI-Tx and SCI-Rx on an interface must be equal.
  – Addition/deletion of keys to/from a keychain already associated with a SCI-Tx and SCI-Rx under MACsec would not be allowed by Security Keychain module. The keychain also cannot be deleted.
  – MACsec cannot be administratively enabled on an interface until both SCI-Tx and SCI-Rx are configured on the interface.
  – The Tx/Rx secure channel cannot be removed without disabling MACsec on the interface.
  – The encryption option on the Tx/Rx channel can either be enabled or disabled. By default, the ‘encryption’ is disabled. Enabling ‘encryption’ option ensures that the data in the Ethernet frame cannot be viewed by anyone monitoring traffic on the link. Use the no form of the command to disable encryption on Tx/Rx channel.
  – MACsec SCI-Tx/SCI-Rx values cannot be updated at run-time. The SCI-Tx/Rx values must be unconfigured and re-configured. Only ‘keychain ID’ and ‘encryption’ parameters can be updated at run-time.
  – During run-time, upon enabling or disabling MACsec on the port, the interface will get re-initialized (interface will be brought down and up), which will result in temporary traffic loss.
  – MACsec mandates specifying SCI-Tx and SCI-Rx value (for configured explicit SCI) while updating its ‘keychain ID’ and ‘encryption’ parameters on an interface.
  – While unconfiguring ‘keychain ID’ and ‘encryption’ parameters on an interface, it is not mandatory to provide MACsec SCI-Tx value, whereas, MACsec mandates specifying SCI-Rx value (for explicit SCI).
For MACsec mode ‘dynamic’ - dynamic SAK using pre-shared keys, following are the configuration guidelines:

- The keychain or pre-shared key for Static-CAK must have the key mapped either to ‘AES-CMAC-128’ algorithm or ‘AES-CMAC-256’ algorithm. AES-CMAC-256 option would be supported only on platforms supporting 256-bit key. View show interfaces capability output to check if the interfaces has the support for MACsec 256-bit encryption.
- If there are multiple pre-shared keys configured in the keychain, only the first key would be used for CAK.
- Key server priority would be in the range 0-255, with lower value having higher precedence.
- Enabling or disabling Encryption enables or disables encryption on dynamic Secure-Channel (SC).

For MACsec mode ‘radius’ - dynamic SAK using EAP, following are the configuration guidelines:

- Dynamic mode using RADIUS server requires the switch end port connecting a host (supplicant) to be enabled with UNP and configured for 802.1x-authentication, and MSK/Key-Name received from Server as part of the authentication. The authentication method must be either EAP-TLS or PEAP authentication framework.
- The switch end port connecting a host (supplicant) must be enabled with UNP and configured for 802.1x-authentication.
- The MACsec mode dynamic on UNP is supported in single supplicant mode only, that is, the UNP port can learn only one supplicant on the MACsec enabled interface. Also, there cannot be any non-suppliant learned on the same port.
- Flushing the supplicant MAC on UNP port would purge the existing MACsec MKA session, (MACSec Key Agreement), and the port would be unsecured until the supplicant is learned again.
- Re-authentication of supplicant may change the UNP profile or VLAN and the policy applied to the MAC. The existing MACsec session established (if any) would remain intact if the re-authentication results in the same MSK/Key-Name from RADIUS server. Otherwise, the existing MKA session would be purged and a new session is established using the new MSK/Key-Name.
- Captive portal authentication, BYOD, and LTP (location/time policy) is not supported on MACsec enabled UNP ports.
- MACsec mode dynamic using ‘radius’ will not be supported on UNP Linkagg.

- Refer to the latest release notes for a detailed list of MACsec platform and module support.

- OmniSwitch 6860(E) and OmniSwitch 6860N models must have encryption enabled when interoperating.

- To confirm the MACsec support on the interface, use the show interfaces capability command. MACsec 128-bit and 256-bit support on a port is listed respectively against the MACsec Supported and Macsec 256-bit fields.

- MACsec must be enabled on all ports (on a per physical port basis) that are part of the same link aggregation.

- MACsec mode cannot be changed if MACsec is already administratively enabled. To change MACsec mode, administratively disable MACsec first.

- ISSU upgrade from previous releases to the latest version is not compatible for MACsec dynamic mode. Hence, it is recommended to run the same version of the AOS image on all the MACsec nodes for MACsec dynamic mode.

- MACsec is supported between two directly connected Service Access Ports or network ports for service type SPB/VXLAN/L2GRE. This is supported only on OmniSwitch 6900-X48C4E, OmniSwitch 6860N, and OmniSwitch 6860E platforms.
• Use the **no** form of this command to disable encryption on Tx/Rx channel, remove keychain configuration on Tx/Rx channel, remove Tx/Rx channel.

**Examples**

-> interface port 1/1/1 macsec admin-state enable mode static sci-Tx 0x1 key-chain 1 encryption sci-rx 0x1 key-chain 1 encryption

-> interface port 1/1/1 macsec admin-state enable mode dynamic key-chain 1 server-priority 10 transmit-interval 3

-> interface port 1/1/1 macsec admin-state enable mode dynamic radius

-> no interface port 1/1/1 macsec sci-rx 0x2 keychain

-> no interface port 1/1/1 macsec sci-tx encryption

**Release History**

Release 8.4.1 R03; command introduced.
Release 8.5R2; Dynamic SA Mode - Dynamic SAK using Pre-Shared Key and Dynamic SAK using EAP support added.

**Related Commands**

- **show interfaces macsec**
  Displays the MACsec configuration on a physical port or port range.
- **show interfaces macsec static**
  Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Static’.
- **show interfaces macsec dynamic**
  Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Dynamic’.
- **show interfaces macsec statistics**
  Displays the MACsec statistics collected for a physical port.

**MIB Objects**

- `alaSecyTxSCTable`
  - `alaSecyTxSCI`
  - `alaSecyTxSCKeyChainId`
  - `alaSecyTxSCEncryption`
- `alaSecyRxSCTable`
  - `alaSecyRxSCI`
  - `alaSecyRxSCKeyChainId`
  - `alaSecyRxSCEncryption`
- `alaSecyIfTable`
  - `alaSecyIfAdminStatus`
  - `alaSecyIfMode`
**interfaces macsec key-rotation max-session-time**

Configures the session timer on a single port or a range of ports to perform a Secure Association Key (SAK) re-generation when the session timer gets expired.

```
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} macsec key-rotation {max-session-time num | default}
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for a specific module.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-10).
- `num` The number of minutes a session lasts before the next rekey. Valid range is 5 minutes - 120 minutes (in the increment of 5 minutes).
- `default` Disable the session time.

**Defaults**

By default, the key rotation session time is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900V72/C32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter a slot and port number or a range of port numbers to configure the timer value for a specific interface or a range of interfaces.
- The SAK re-generation is performed at the key server side when the session time reaches the configured limit. In addition, the session time on the port is reset to the configured value.
- The configuration must be configured on both ends of the MACsec enabled interface as either of the sides can be elected as the key server.
- By default, key rotation happens when the Packet Number reaches 0xC0000000 if key rotation is not configured.
- When max-session-time is configured, if the Packet Number reaches 3/4th PN expiry (0xC0000000) or the exchange data reaches the configured limit before the session-time gets expired, the key will still get rotated. In addition, the session time on the port is reset to the configured value.
- Disabling MACsec stops the session timer.
**Examples**

-> interface port 1/1/1 macsec key-rotation max-session-time 20

**Release History**

Release 8.9R1; command introduced.

**Related Commands**

- `show interfaces macsec` Displays the MACsec configuration on a physical port or port range.
- `show interfaces macsec dynamic key-rotation` Displays the remaining session time and the exchanged data on the MACsec interfaces.

**MIB Objects**

alaSecyIfTable
alaSecySessionTime
interfaces macsec key-rotation max-exchange-data

Configures the data exchange on a single port or a range of ports to perform a SAK re-generation each time the limit is reached. This is the data exchanged (received or transmitted) between the MACsec endpoints.

```
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} macsec key-rotation {max-exchange-data num [M(mega)|G(giga)] | default}
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.
- **slot**
  - The slot number for a specific module.
- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-10).
- **num**
  - The amount of GB data exchanged before the next key re-generation. Valid range is 10M (bytes) – 1000G (bytes). MB is the default value. Configuration allowed in increments like below:
    - 10M, 20M... with 10MB increment
    - 100M, 200M, with 100M increment
    - 1G, 2G, .... with 1GB increment till 100G.
- **default**
  - Disable the data exchange.

### Defaults

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>default, which means the data-exchange is disabled.</td>
</tr>
</tbody>
</table>
```

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C4E</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a slot and port number or a range of port numbers to configure the data exchange value for a specific interface or a range of interfaces.
- The SAK re-generation is performed at key server side when the exchanged data reaches the configured value if the key life is less than two minutes.
- The configuration must be configured on both ends of the MACsec enabled interface as either of the sides can be elected as the key server.
• By default, key rotation happens when the Packet Number reaches 0xC0000000 if key rotation is not configured.

• When max-exchange-data is configured, if the Packet Number reaches 3/4th PN expiry (0xC0000000) or the session time gets expired before reaching the configured exchange data, the key will still get rotated. In addition, the count of exchange data on the port is reset to the configured value.

**Examples**

```
-> interface port 1/1/5 macsec key-rotation max-exchange-data 10M
-> interface port 1/1/5 macsec key-rotation max-exchange-data 1G
```

**Release History**

Release 8.9R1; command introduced.

**Related Commands**

```
show interfaces macsec
  Displays the MACsec configuration on a physical port or port range.

show interfaces macsec dynamic key-rotation
  Displays the remaining session time and the exchanged data on the MACsec interfaces.
```

**MIB Objects**

```
alaSecyIfTable
  alaSecyExchangeData
```
**show interfaces macsec**

Displays the MACsec configuration on a physical port or port range.

`show interfaces macsec [chassis/slot/port[-port2]]`

**Syntax Definitions**

`chassis`    The chassis identifier.

`slot`       Slot number to display information about all ports on a specific slot.

`port[-port2]`  The port number of a specific interface to display. Use a hyphen to specify a range of ports.

**Defaults**

By default, the MACsec configuration on all ports is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C4E</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enter a port number with this command to display the MACsec configuration for a specific port.

**Examples**

`-> show interfaces macsec`

<table>
<thead>
<tr>
<th>Chas/Slot/Port</th>
<th>Admin-State</th>
<th>Mode</th>
<th>Encryption</th>
<th>Session Time (Min)</th>
<th>Exchange Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Enabled</td>
<td>Static</td>
<td>Enabled</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Enabled</td>
<td>Dynamic</td>
<td>Enabled</td>
<td>20</td>
<td>-</td>
</tr>
<tr>
<td>1/1/4</td>
<td>Enabled</td>
<td>Dynamic</td>
<td>Enabled</td>
<td>-</td>
<td>1000G</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Enabled</td>
<td>Dynamic</td>
<td>Disabled</td>
<td>60</td>
<td>500</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chas/Slot/Port</td>
<td>The chassis/slot/port identifier.</td>
</tr>
<tr>
<td>Admin-State</td>
<td>The interface administrative status.</td>
</tr>
<tr>
<td>Mode</td>
<td>The MACsec mode.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Status of encryption on Tx/Rx channel.</td>
</tr>
<tr>
<td></td>
<td>Encryption field will display &quot;Enabled&quot; or &quot;Disabled&quot; if it is enabled or</td>
</tr>
<tr>
<td></td>
<td>disabled respectively on both Tx/Rx. However, if encryption is enabled</td>
</tr>
<tr>
<td></td>
<td>only on Tx or only on Rx, it would be disabled as &quot;Tx Enabled&quot; or &quot;Rx</td>
</tr>
<tr>
<td></td>
<td>Enabled&quot; respectively.</td>
</tr>
<tr>
<td>Session Time (Min)</td>
<td>The maximum session time configured on a single port or a range of ports to</td>
</tr>
<tr>
<td></td>
<td>perform a SAK re-generation.</td>
</tr>
<tr>
<td>Exchange Data</td>
<td>The maximum data exchange configured on a single port or a range of ports to</td>
</tr>
<tr>
<td></td>
<td>perform a SAK re-generation.</td>
</tr>
</tbody>
</table>

Release History

Release 8.4.1.R03; command introduced.
Release 8.9R1; Session Time (Min), Exchange Data fields added.

Related Commands

interfaces macsec admin-state  Enables or disables MACsec on a physical port or a port range.

MIB Objects

alaSecyIfTable
   alaSecyIfAdminStatus
   alaSecyIfMode
alaSecyTxSCTable
   alaSecyTxSCEncryption
alaSecyRxSCTable
   alaSecyRxSCEncryption
show interfaces macsec static

Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Static’.

show interfaces macsec static [chassis/slot/port[-port2]]

Syntax Definitions

chassis The chassis identifier.

slot Slot number to display information about all ports on a specific slot.

port[-port2] The port number of a specific interface to display. Use a hyphen to specify a range of ports.

Defaults

By default, the detailed MACsec configuration on all ports is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C4E</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enter a port number with this command to display the detailed MACsec configuration for a specific port.

Examples

-> show interfaces macsec static
Chas/Slot/Port Admin-State SCI Type Keychain Encryption
-----------------------------------------------+---------+----------+-----+----------------+------------+
 1/1/1  Enabled   0x0000000000000001 TX 1   Enabled
 1/1/1  Enabled   0x0000000000000002 RX 1   Enabled
 1/1/2  Disabled  -      TX 2   Disabled
 1/1/2  Disabled  -      RX 2   Disabled
 1/1/3  Disabled  0x0000000000000003 TX 3   Enabled
 1/1/3  Disabled  0x0000000000000004 RX 3   Disabled

-> show interfaces macsec static 1/1/1
Chas/Slot/Port Admin-State SCI Type Keychain Encryption
-----------------------------------------------+---------+----------+-----+----------------+------------+
 1/1/1  Enabled   0x0000000000000001 TX 1   Disabled
 1/1/1  Enabled   0x0000000000000002 RX 1   Disabled
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chas/Slot/Port</td>
<td>The chassis/slot/port identifier.</td>
</tr>
<tr>
<td>Admin-State</td>
<td>The interface administrative status.</td>
</tr>
<tr>
<td>SCI</td>
<td>The configured SCI value for Tx and Rx channel in the hexadecimal format (0xhex).</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the secure channel type: Tx/Rx</td>
</tr>
<tr>
<td>Keychain</td>
<td>The keychain ID associated to Tx/Rx channel.</td>
</tr>
<tr>
<td>Mode</td>
<td>The MACsec mode.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Status of encryption on Tx/Rx channel.</td>
</tr>
</tbody>
</table>

Release History

Release 8.4.1 R03; command introduced.

Related Commands

- **interfaces macsec admin-state**  Enables or disables MACsec on a physical port or a port range.

MIB Objects

- **alaSecyTxSCTable**
  - **alaSecyTxSCI**
  - **alaSecyTxSCKeyChainId**
  - **alaSecyTxSCEncryption**

- **alaSecyRxSCTable**
  - **alaSecyRxSCI**
  - **alaSecyRxSCKeyChainId**
  - **alaSecyRxSCEncryption**

- **alaSecyIfTable**
  - **alaSecyIfAdminStatus**
  - **alaSecyIfMode**
show interfaces macsec dynamic

Displays the detailed MACsec configuration on a physical port or port range configured with MACsec mode ‘Dynamic’.

show interfaces macsec dynamic [details] [chassis/slot/port[-port2]]

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: Slot number to display information about all ports on a specific slot.
- **port[-port2]**: The port number of a specific interface to display. Use a hyphen to specify a range of ports.

**Defaults**

By default, the detailed MACsec configuration on all ports is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

| Platform | Support
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enter a port number with this command to display the detailed MACsec configuration for a specific port.

**Examples**

-> show interface macsec dynamic

<table>
<thead>
<tr>
<th>Chas/Slot/Port</th>
<th>Admin-State</th>
<th>Mode</th>
<th>Keychain</th>
<th>Encryption</th>
<th>Server Priority</th>
<th>Transmit Interval(Sec)</th>
<th>Key Server</th>
<th>Operation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Enabled</td>
<td>keychain</td>
<td>2</td>
<td>Enabled</td>
<td>10</td>
<td>3</td>
<td>YES</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>1/1/3</td>
<td>Enabled</td>
<td>keychain</td>
<td>1</td>
<td>Disabled</td>
<td>12</td>
<td>2</td>
<td>YES</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>1/1/4</td>
<td>Enabled</td>
<td>keychain</td>
<td>1</td>
<td>Disabled</td>
<td>13</td>
<td>5</td>
<td>NO</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>1/1/5</td>
<td>Enabled</td>
<td>radius</td>
<td>NA</td>
<td>Disabled</td>
<td>14</td>
<td>6</td>
<td>NO</td>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>

-> show interface macsec dynamic 1/1/3-4

<table>
<thead>
<tr>
<th>Chas/Slot/Port</th>
<th>Admin-State</th>
<th>Mode</th>
<th>Keychain</th>
<th>Encryption</th>
<th>Server Priority</th>
<th>Transmit Interval(Sec)</th>
<th>Key Server</th>
<th>Operation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/3</td>
<td>Enabled</td>
<td>keychain</td>
<td>1</td>
<td>Disabled</td>
<td>12</td>
<td>2</td>
<td>YES</td>
<td>UP</td>
<td></td>
</tr>
<tr>
<td>1/1/4</td>
<td>Enabled</td>
<td>keychain</td>
<td>1</td>
<td>Disabled</td>
<td>13</td>
<td>5</td>
<td>NO</td>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>

-> show interface macsec dynamic 1/1/5

<table>
<thead>
<tr>
<th>Chas/Slot/Port</th>
<th>Admin-State</th>
<th>Mode</th>
<th>Keychain</th>
<th>Encryption</th>
<th>Server Priority</th>
<th>Transmit Interval(Sec)</th>
<th>Key Server</th>
<th>Operation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/5</td>
<td>Enabled</td>
<td>radius</td>
<td>NA</td>
<td>Disabled</td>
<td>14</td>
<td>6</td>
<td>NO</td>
<td>UP</td>
<td></td>
</tr>
</tbody>
</table>
-> show interfaces macsec dynamic details 1/1/3-4

<table>
<thead>
<tr>
<th>Chas/Slot/Port</th>
<th>SCI</th>
<th>Type</th>
<th>In-used SA</th>
<th>PN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/3</td>
<td>0x0000000000000001</td>
<td>TX</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>1/1/3</td>
<td>0x0000000000000002</td>
<td>RX</td>
<td>1</td>
<td>50</td>
</tr>
<tr>
<td>1/1/4</td>
<td>0x0000000000000003</td>
<td>TX</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>1/1/4</td>
<td>0x0000000000000004</td>
<td>RX</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>1/1/5</td>
<td>0x0000000000000005</td>
<td>TX</td>
<td>0</td>
<td>40</td>
</tr>
<tr>
<td>1/1/5</td>
<td>0x0000000000000006</td>
<td>RX</td>
<td>1</td>
<td>50</td>
</tr>
</tbody>
</table>

-> show interfaces macsec dynamic details 1/1/4

<table>
<thead>
<tr>
<th>Chas/Slot/Port</th>
<th>SCI</th>
<th>Type</th>
<th>In-use SA</th>
<th>PN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/4</td>
<td>0x0000000000000003</td>
<td>TX</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>1/1/4</td>
<td>0x0000000000000004</td>
<td>RX</td>
<td>1</td>
<td>30</td>
</tr>
</tbody>
</table>

output definitions

- **Chas/Slot/Port**: The chassis/slot/port identifier.
- **Admin-State**: The interface administrative status.
- **Mode**: The MACsec mode. ‘Keychain’, ‘Radius’ keyword denotes dynamic MACsec using pre-shared key or EAP (RADIUS server) respectively.
- **Keychain**: The keychain ID associated to Tx/Rx channel.
- **Encryption**: Status of encryption on Tx/Rx channel.
- **Server Priority**: The priority configured for the key server.
- **Transmit Interval(Sec)**: The transmit interval configured for MKPDU (in seconds).
- **Key Server**: Indicates the key server.
- **Operation Status**: The MACsec operational status.
- **SCI**: The SCI value dynamically generated for Tx and Rx channel in the hexadecimal format (0xhex).
- **Type**: Specifies the secure channel type: Tx/Rx.
- **In-use SA**: Identifier for currently active Association Number (SA) in use for Tx/Rx channel on the interface.
- **PN**: The packet number of the last packet received on the MACsec interface.

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- **interfaces macsec admin-state**: Enables or disables MACsec on a physical port or a port range.

**MIB Objects**

- **N/A**
**show interfaces macsec statistics**

Displays the MACsec statistics collected for a physical port.

```
show interfaces macsec statistics [chassis/slot/port|-port]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot</td>
<td>Slot number to display information about all ports on a specific slot.</td>
</tr>
<tr>
<td>port[-port]</td>
<td>The port number of a specific interface to display. Use a hyphen to specify a range of ports.</td>
</tr>
</tbody>
</table>

### Defaults

- If chassis/slot/port is not specified, the output will be displayed in tabular format but only important statistics will be displayed.

- If chassis/slot/port is specified, the output will not be displayed in tabular format but all statistics will be displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T48C6/X48C4E</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T48C6/X48C4E</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T48C6/X48C4E</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show interfaces macsec statistics
Chassis/Slot/Port 1/1/3
Byte Transmitted : 21035280, Untagged TX Pkts : 0
Too Long TX Pkts : 0, Byte Received : 0
Untagged RX Pkts : 0, No Tagged RX Pkts : 466
Bad Tagged RX Pkts : 0, Unknown SCI RX Pkts : 0
No SCI RX Pkts : 0, Overrun RX Pkts : 0
SCI-TX: 0x0000000000000001
```
Ethernet Port Commands

show interfaces macsec statistics

TX Protected Pkts : 0, TX Encrypted Pkts : 0
TX Octets Protected : 487920, TX Octets Encrypted : 16340448
SA: 0
  TX Protected Pkts : 10165, TX Encrypted Pkts : 340427
  SA: 1
    TX Protected Pkts : 0, TX Encrypted Pkts : 0
SCI-RX: 0x0000000000000000
RX Unused SA Pkts : 0, RX No Using SA Pkts : 0
RX Late Pkts : 0, RX Not Valid Pkts : 0
RX Invalid Pkts : 0, RX Delayed Pkts : 0
RX Unchecked Pkts : 0, RX OK Pkts : 0
RX Octets Validated : 0, RX Octets Decrypted : 0
SA: 0
  RX Unused SA Pkts : 0, RX No Using SA Pkts : 0
  RX Not Valid Pkts : 0, RX Invalid Pkts : 0
  RX OK Pkts : 0
SA: 1
  RX Unused SA Pkts : 0, RX No Using SA Pkts : 0
  RX Not Valid Pkts : 0, RX Invalid Pkts : 0
  RX OK Pkts : 0s...

output definitions

Chas/Slot/Port
Interface chassis, slot and port.
Bytes Xmitted
Number of Bytes transmitted.
TX Untagged Pkts
Number of untagged packets transmitted.
TX Too-Long Pkts
Number of long packets transmitted.
Bytes Received
Number of Bytes received.
RX Untagged Pkts
Number of untagged packets received.
RX Bad-Tag Pkts
Number of bad tag packets received.
Unknown SCI RX Pkts
Number of unknown packets received.
Overrun RX Pkts
Number of packets overrun.
TX Protected Pkts
Number of protected packets transmitted.
TX Encrypted Pkts
Number of encrypted packets transmitted.
TX Octets Protected
Number of packets protected in each listed octet range.
TX Octets Encrypted
Number of packets encrypted in each listed octet range.
RX Unused SA Pkts
Number of unused SA packets received.
RX No Using SA Pkts
Number of SA packets not used.
RX Late Pkts
Number of late packets received.
RX Not Valid Pkts
Number of discarded packets.
RX Invalid Pkts
Number of invalid packets.
RX Delayed Pkts
Number of delayed packets received.
RX Unchecked Pkts
Number of unchecked packets received.
RX OK Pkts
Number of valid packets.
RX Octets Validated
Number of packets validated in each listed octet range.
RX Octets Decrypted
Number of packets decrypted in each listed octet range.
Release History

Release 8.4.1 R03; command introduced.

Related Commands

*interfaces macsec admin-state* Enables or disables MACsec on a physical port or a port range.

MIB Objects

```plaintext
secyTxSAStatsTable
  secyTxSAStatsProtectedPkts
  secyTxSAStatsEncryptedPkts

secyTxSCStatsTable
  secyTxSCStatsProtectedPkts
  secyTxSCStatsEncryptedPkts
  secyTxSCStatsOctetsProtected
  secyTxSCStatsOctetsEncrypted

secyRxSAStatsTable
  secyRxSAStatsUnusedSAPkts
  secyRxSAStatsNoUsingSAPkts
  secyRxSAStatsNotValidPkts
  secyRxSAStatsInvalidPkts
  secyRxSAStatsOKPkt

secyRxSCStatsTable
  secyRxSCStatsUnusedSAPkts
  secyRxSCStatsNoUsingSAPkts
  secyRxSCStatsLatePkts
  secyRxSCStatsNotValidPkts
  secyRxSCStatsInvalidPkts
  secyRxSCStatsDelayedPkts
  secyRxSCStatsUncheckedPkts
  secyRxSCStatsOKPkt
  secyRxSCStatsOctetsValidated
  secyRxSCStatsOctetsDecrypted

secyStatsTable
  secyStatsTxUntaggedPkts
  secyStatsTxTooLongPkts
  secyStatsRxUntaggedPkts
  secyStatsRxNoTagPkts
  secyStatsRxBadTagPkts
  secyStatsRxUnknownSIPkts
  secyStatsRxNoSIPkts
  secyStatsRxOverrunPkts
```
show interfaces macsec dynamic key-rotation

Displays the remaining session time and the exchanged data on the MACsec interfaces.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C4E</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the session time and the exchanged data remaining on the MACsec interfaces. This information is available only at the key server side.

**Examples**

```plaintext
-> show interfaces macsec dynamic key-rotation
Chas/Slot/Port   Time to Rekey (Sec)   Data to Rekey (Byte)
---------------------------------------------------------------------
1/1/9            3594                  19999999814
2/1/9            1632                  19869941586
```

**output definitions**

- **Chas/Slot/Port**: The chassis/slot/port identifier.
- **Admin-State**: The interface administrative status.
- **Time to Rekey (Sec)**: The session time remaining on the MACsec interface before key re-generation.
- **Data to Rekey (Byte)**: The exchange data remaining on the MACsec interface before key re-generation.

**Release History**

Release 8.9R1; command introduced.
**Related Commands**

**interfaces macsec key-rotation max-session-time**
Configures the session timer on a single port or a range of ports to perform a Secure Association Key (SAK) re-generation each time the timeout is reached.

**interfaces macsec key-rotation max-exchange-data**
Configures the data exchange on a single port or a range of ports to perform a SAK re-generation each time the limit is reached.

**MIB Objects**

alaSecyRekeyStatusTable
  alaSecyRemainingRekeyTime
  alaSecyRemainingRekeyVolume
clear interfaces macsec statistics

Clears the MACsec statistics globally on all MACsec enabled interfaces.

clear interfaces {slot chassis/slot | port [chassis/slot/port [-port2] | all] macsec-statistics

### Syntax Definitions

- **chassis**
  - The chassis identifier.
- **slot**
  - Slot number to display information about all ports on a specific slot.
- **port[-port2]**
  - The port number of a specific interface to display. Use a hyphen to specify a range of ports.
- **all**
  - Displays information on all MACsec enabled interfaces.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C4E</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is used to clear MACsec statistics on a slot, port, port-range, or on all interfaces globally.

### Examples

- `-> clear interface port 1/1/1 macsec-statistics`
- `-> clear interface port 1/1/1-2 macsec-statistics`
- `-> clear interface slot 1/1 macsec-statistics`
- `-> clear interface all macsec-statistics`

### Release History

- Release 8.4.1 R03; command introduced.
- Release 8.5 R1; **all** keyword added.
Related Commands

`interfaces macsec admin-state` Enables or disables MACsec on a physical port or a port range.

MIB Objects

`alaSecyIfTable`
  `alaSecyIfPortClearStats`
2 Power over Ethernet (PoE) Commands

The Power over Ethernet (PoE) feature is supported on OmniSwitch PoE-capable switches. Refer to the OmniSwitch Hardware Users Guide for further details.

**Note on Terminology.** There are several general terms used to describe this feature. The terms Power over Ethernet (PoE), Power over LAN (PoL), Power on LAN (PoL), and Inline Power are synonymous terms used to describe the powering of attached devices via Ethernet ports. For consistency, this chapter and the OmniSwitch AOS Release 8 CLI Reference Guide refer to the feature as Power over Ethernet (PoE).

Additional terms, such as Powered Device (PD) and Power Source Equipment (PSE) are terms that are not synonymous, but are directly related to PoE.

- **PD** refers to any attached device that uses a PoE data cable as its only source of power. Examples include access points such as IP telephones, Ethernet hubs, wireless LAN stations, etc.
- **PSE** refers to the actual hardware source of the electrical current for PoE (e.g., OmniSwitch PoE-capable switches).

PoE commands documented in this section comply with IEEE 802.3, 802.af, and 802.3at.

MIB information for the PoE commands is as follows:

- **Filename**: ALCATEL-IND1-INLINE-POWER-MIB.mib
- **Module**: alcatelIND1INLINEPOWERMIB

- **Filename**: POWER-ETHERNET-MIB.mib
- **Module**: powerEthernetMIB
A summary of the available commands is listed here:

```plaintext
lanpower service
lanpower port admin-state
lanpower type
lanpower power
lanpower maxpower
lanpower priority
lanpower ni-priority
lanpower priority-disconnect
lanpower power-rule
lanpower power-policy
lanpower class-detection
lanpower capacitor-detection
lanpower usage-threshold
lanpower dynamic-power-mgmt
lanpower update-from
lanpower 4pair
lanpower power-over-hdmi
lanpower 802.3bt
lanpower fpoe
lanpower ppoe
lanpower high-resistance-detection
lanpower trust
show lanpower
show lanpower power-rule
show lanpower power-policy
show lanpower class-detection
show lanpower capacitor-detection
show lanpower priority-disconnect
show lanpower ni-priority
show lanpower usage-threshold
show lanpower firmware-upgrade-status
show lanpower high-resistance-detection
show lanpower status
```
**lanpower service**

Activates or stops PoE service on all ports in a specified slot.

```
lanpower {chassis chassis | slot chassis/slot} service {start | stop}
```

**Syntax Definitions**

- **chassis**
  The chassis on which the PoE power is being turned on or off.

- **chassis/slot**
  The slot on which the PoE power is being turned on or off.

- **start**
  Activates PoE on all ports in the specified slot.

- **stop**
  Turns off PoE on all ports in the specified slot.

**Defaults**

Power over Ethernet is globally disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The OmniSwitch 6465 cannot auto-detect the type of power supply connected. The type of power supply connected must be configured so that the system and PoE power information is correctly displayed and utilized. Use the `powersupply type` type command to configure the power supply.

**Examples**

```
-> lanpower slot 2/1 service start
-> lanpower chassis 1 service stop
```

**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.
Related Commands

- `lanpower port admin-state` Activates or stops PoE service on an individual port.
- `show lanpower` Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

- `alaPethMainPseTable`
  - `alaPethMainPseAdminStatus`
**lanpower port admin-state**

Activates or stops PoE service on an individual port.

`lanpower port chassis/slot/port admin-state {enable | disable}`

---

**Syntax Definitions**

- **chassis/slot/port** The individual port on which the PoE power is being turned on or off.
- **enable** Activates PoE on the specified port.
- **stop** Turns off PoE on the specified port.

**Defaults**

Power over Ethernet is globally disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `-> lanpower port 2/1/1 admin-state enable`
- `-> lanpower port 1/1/12 admin-state disable`

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `lanpower service` Activates or stops PoE service on all ports in a specified slot.
- `show lanpower` Displays the PoE status and related statistics for all ports in a specified slot.

**MIB Objects**

- `pethPsePortTable`
  - `pethPsePortAdminEnable`
**lanpower type**

Assigns a user-defined port type to a specific port (when `chassis/slot/port` values are entered) or across all ports in a chassis or slot.

```plaintext
lanpower {chassis chassis | slot chassis/slot | port chassis/slot/port} type string
```

**Syntax Definitions**

- `chassis`  The chassis on which a port type is being defined.
- `chassis/slot`  The slot on which a port type is being defined.
- `chassis/slot/port`  The specific port on which a port type is being defined.
- `string`  A user-defined text string of up to nine (9) characters. This text string will be listed in the "Type" column in the `lanpower update-from` command output.

**Defaults**

Refer to the `OmniSwitch Hardware Users Guide` for default power settings.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is not supported when using PoE 3.xx (802.3bt) firmware. Firmware 3.xx automatically enables class-detection and does not allow per port power limits to be configured.

- Using this command does not immediately allocate the power to the slot or port. Any unused power is still available and remains a part of the overall PoE budget.

- To globally specify the amount of inline power available to all ports in a slot, refer to the `lanpower maxpower` command on page 2-8.

- Be sure that the value specified complies with specific power requirements for all attached PDs.

- Note that the power value for the `lanpower power` command is specified in milliwatts (mW); the related command, `lanpower maxpower`, is specified in watts (W).

**Examples**

- `-> lanpower slot 3/1 power 3200`
- `-> lanpower port 1/1/24 power 25000`
- `-> lanpower chassis 1 power 3000`
**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

**Related Commands**

- **lanpower maxpower**
  Specifies the maximum amount of inline power, in watts, available to all PoE ports in a specified slot.

- **show lanpower**
  Displays the PoE status and related statistics for all ports in a specified slot.

**MIB Objects**

`alaPethPsePortTable`

  - `alaPethPsePortPowerMaximum`
**lanpower maxpower**

Specifies the maximum amount of power, in watts, assigned to a specified slot.

```
lanpower {chassis chassis | slot chassis/slot} maxpower {watts | default}
```

### Syntax Definitions

- **chassis**
  The chassis containing PoE ports on which the maximum amount of inline power allowed is being configured.

- **chassis/slot**
  The slot containing PoE ports on which the maximum amount of inline power allowed is being configured.

- **watts**
  The maximum amount of inline power, in watts, available to all PoE ports in the corresponding slot. Refer to the *OmniSwitch Hardware Users Guide* for additional PoE specifications.

- **default**
  Sets the power value back to the default setting.

### Defaults

<table>
<thead>
<tr>
<th>installed power supply</th>
<th>default</th>
<th>range</th>
</tr>
</thead>
<tbody>
<tr>
<td>920W Power Supply (OS6860)</td>
<td>780W</td>
<td>37-780</td>
</tr>
<tr>
<td>600W Power Supply (OS6860)</td>
<td>450W</td>
<td>37-450</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- To specify the maximum amount of inline power available to a single port, refer to the *lanpower power*.

- Note that the power value for the *lanpower maxpower* command is specified in watts (W); the related command, *lanpower power*, is specified in milliwatts (mW).

### Examples

- `-> lanpower slot 3/1 maxpower 400`
- `-> lanpower chassis 1 maxpower 400`
**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.
Release 8.8R1; **default** parameter added.

**Related Commands**

- **`lanpower power`**
  Specifies the amount of power, in milliwatts, provided for a specific port (when `chassis/slot/port` values are entered) or across all ports in a slot (if only `slot/port` values are entered).

- **`show lanpower`**
  Displays the PoE status and related statistics for all ports in a specified slot.

**MIB Objects**

- `alaPethMainPseTable`
  - `alaPethMainPseMaxPower`
**lanpower priority**

Specifies PoE power priority level to a port (when *chassis/slot/port* values are entered) or across all ports in a slot (if only *slot/port* values are entered). Levels include critical, high, and low.

```
lanpower {chassis chassis | slot chassis/slot | port chassis/slot/port} priority {critical | high | low}
```

**Syntax Definitions**

- **chassis**
  - The chassis on which the PoE power priority is being set.
- **chassis/slot**
  - The slot on which the PoE power priority is being set.
- **chassis/slot/port**
  - The specific port on which the PoE power priority is being set.
- **critical**
  - Intended for ports that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, power to critical ports is maintained as long as possible.
- **high**
  - Intended for ports that have important, but not mission-critical, devices attached. If other ports in the chassis have been configured as critical, power to high-priority ports is given second priority to critical devices.
- **low**
  - Intended for ports that have low-priority devices attached. In the event of a power management issue, power to low-priority ports is interrupted first (i.e., before critical- and high-priority ports).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>high</td>
</tr>
<tr>
<td>low</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power. For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power.

**Examples**

- `-> lanpower slot 2/1 priority low`
- `-> lanpower port 1/1/6 priority critical`
-> lanpower chassis 1 priority low

**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

**Related Commands**

- **lanpower priority-disconnect**: Enables or disables the priority disconnect function on all ports in a specified slot.
- **show lanpower**: Displays the PoE status and related statistics for all ports in a specified slot.

**MIB Objects**

- pethPsePortTable
  - pethPsePortPowerPriority
**lanpower ni-priority**

Specifies power priority level to a Network Interface (NI) module. Levels include critical, high, and low.

`lanpower {chassis chassis | slot chassis/slot} ni-priority {critical | high | low}`

### Syntax Definitions

- **chassis**
  The chassis on which the NI priority is being set.

- **chassis/slot**
  The slot on which the NI priority is being set.

- **critical**
  Intended for modules that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, power to critical NIs is maintained as long as possible.

- **high**
  Intended for modules that have important, but not mission-critical, devices attached. If other NIs in the chassis have been configured as critical, power to high-priority modules is given second priority to critical devices.

- **low**
  Intended for modules that have low-priority devices attached. In the event of a power management issue, power to low-priority modules is interrupted first (i.e., before critical- and high-priority NIs).

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>high</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power. For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power.

### Examples

- `-> lanpower slot 2/1 ni-priority low`
- `-> lanpower chassis 1 ni-priority low`
Release History
Release 8.3.1; command was introduced.

Related Commands

show lanpower ni-priority
Displays current Network Interface (NI) modules status for a specified chassis or slot.

MIB Objects
N/A
**lanpower priority-disconnect**

Enables or disables the priority disconnect function on all ports in a specified slot. Priority disconnect is used by the system software in determining whether an incoming PD will be granted or denied power when there are too few watts remaining in the PoE power budget for an additional device.

```
lanpower {chassis chassis | slot chassis/slot} priority-disconnect {enable | disable}
```

**Syntax Definitions**

- `chassis` The chassis on which the priority disconnect function is being enabled or disabled.
- `chassis/slot` The particular slot on which the priority disconnect function is being enabled or disabled.
- `enable` Enables priority disconnect on a specified port. When this function is enabled and a power budget deficit occurs in which there is inadequate power for an incoming device, the system software uses priority disconnect rules to determine whether an incoming device will be granted or denied power.
- `disable` Disables priority disconnect on a specified port. When priority disconnect is disabled and there is inadequate power in the budget for an additional device, power will be denied to any incoming PD, regardless of its priority status.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power (per power supply installed). For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power (per power supply installed).

**Examples**

```
-> lanpower slot 2/1 priority-disconnect enable
-> lanpower chassis 1 priority-disconnect disable
```
Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

**lanpower priority**

Specifies PoE power priority level to a port (when *chassis/slot/port* values are entered) or across all ports in a slot (if only *slot/port* values are entered).

**lanpower update-from**

Displays the PoE status and related statistics for all ports in a specified slot.

**show lanpower priority-disconnect**

Displays current priority disconnect status for a specified slot.

MIB Objects

alaPethMainPseTable

alaPethMainPsePriorityDisconnect
**lanpower power-rule**

Specifies user-defined power rules that can be assigned to PoE ports.

```
lanpower power-rule rule-name [admin-state {enable | disable}] [power {on | off}] [at {minutes mm | time hh:mm}] [days {all | day [day...] | date [date...] | months {all | month}] [timezone {local-server | utc | originator-server}]
```

```
no lanpower power-rule rule-name [admin-state {enable | disable}] [power {on | off}] [at {minutes mm | time hh:mm}] [days {all | day [day...] | date [date...] | months {all | month}] [timezone {local-server | utc | originator-server}]
```

---

**Syntax Definitions**

- **rule-name**: A user-defined name (up to 32 characters) for the power rule being configured.

- **admin-state**: Specifies the admin-state for the power rule.
  - **enable**: Enables the power rule.
  - **disable**: Disables the power rule.

- **power**: Specifies the power status (on or off) for devices connected to ports within the power rule.
  - **on**: Powers on devices on ports for which the rule is assigned.
  - **off**: Powers off devices on ports for which the rule is assigned.

- **at**: Activates a power rule timer. Power rules are triggered on a specified date or day of the week or at a particular time, or after a specified amount of time has elapsed.
  - **minutes**: Sets a timer. Power rules will take effect when a specified number of minutes have elapsed.
  - **mm**: The number of minutes that will elapse before the power rules take effect.
  - **time**: Sets a timer. Power rules will take effect at a specified time of day.
    - **hh:mm**: The time of day that the power rule will take effect.

- **days**: Specifies that the power rule will take effect on a particular day of the week.
  - **all**: Specifies that the power rule will take effect on all days of the week (Monday through Sunday).
  - **day**: Specifies a particular day of the month or week the power rule will take effect. When entering a day of the month, enter one or more numbers from 1 to 31. When entering a day of the week, use three-digit abbreviations (e.g., **mon**, **tue**, **wed**, **thu**, **fri**, **sat** and **sun**). Any combination of days may be entered in any order. Refer to command line examples for more information.

- **month**: Specifies that the power rule will take effect during a particular month.
  - **all**: Specifies that the power rule will take effect during all months of the year (January through December).
**month**

Specifies a particular month of the year the power rule will take effect. When entering a month, use three-digit abbreviations (e.g., `jan`, `feb`, `mar`, `apr`, `may`, `jun`, `jul`, `aug`, `sep`, `oct`, `nov` and `dec`). Any combination of months may be entered in any order. Refer to command line examples for more information.

**timezone**

Sets a timezone in which timer-based power rules will take effect.

**local-server**

Time as specified by a local server.

**utc**

Specifies that timer-based rules fall under Universal Time Coordinated (UTC) time.

**originator-server**

Time as specified via the network.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Before a power rule can take effect, the rule must first be assigned to particular slots or ports via the `lanpower power-policy` command.

- Timers are created based on the current system time. If the system time is changed the rules must be recreated.

**Examples**

- `-> lanpower power-rule RuleTest2 admin-state enable power on at minutes 10 days fri thu tue months all timezone utc`
- `-> lanpower power-rule new power on at time 18:30 days all months all timezone utc`
- `-> lanpower power-rule OutgoingPDs power off at time 6:00 days 1 2 3 6 9 12 31 months all timezone utc`
- `-> lanpower power-rule NewRule admin-state enable power off at minutes 4 days all months all timezone utc`

**Release History**

Release 8.1.1; command was introduced.
**Related Commands**

- **lanpower power-policy**
  Allows users to bind existing power rules to particular slots or ports.

- **show lanpower power-rule**
  Displays current PoE power rule settings.

- **show lanpower power-policy**
  Displays existing power policies assigned to a slot, port or rule.

**MIB Objects**

- **alaPethPowerRuleTable**
  - **alaPethPowerRuleAdminStatus**
  - **alaPethPowerRulePowerStatus**
  - **alaPethPowerRuleAtMinute**
  - **alaPethPowerRuleAtTime**
  - **alaPethPowerRuleDaysOfMonth**
  - **alaPethPowerRuleDaysOfWeek**
  - **alaPethPowerRuleMonths**
  - **alaPethPowerRuleTimezone**
  - **alaPethPowerRuleRowStatus**
**lanpower power-policy**

Allows users to bind existing power rules to particular slots or ports.

```
lanpower [slot chassis/slot | port chassis/slot/port-port] power-policy policy-name [power-rule rule-name]
```

```
no lanpower power-policy name
no lanpower [slot chassis/slot | port chassis/slot/port-port] power-policy
```

---

**Syntax Definitions**

- **chassis/slot**: The slot on which the power policy (with its associated power rule) is being assigned. This syntax is used the first time the `lanpower power-policy` command is entered, where a policy is being assigned to a particular slot. See Usage Guidelines below for more information.

- **chassis/slot/port-port**: The specific slot on which the power policy (with its associated power rule) is being assigned. Port values may be entered as a single port or range of ports. This syntax is used the first time the `lanpower power-policy` command is entered, where a policy is being assigned to a particular slot. See Usage Guidelines below for more information.

- **policy-name**: A user-defined name (up to 32 characters) for the power policy being configured (or assigned to an existing power rule).

- **rule-name**: This syntax is used the second time the `lanpower power-policy` command is entered, where a policy is being assigned to an existing power rule. See Usage Guidelines below for more information.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- One or more power rules must be created before using the `lanpower power-policy` command. For information on creating power rules, see the `lanpower power-rule` command on page 2-16.

- Using the `lanpower power-policy` command is a two-step process. First, use the command to assign the policy to specific slots or ports. For example:

  ```
  -> lanpower slot 1/1 power-policy NewPolicy
  -> lanpower port 1/1/23 power-policy NewPolicy
  ```
-> lanpower port 1/1/1-12 power-policy NewPolicy

Next, run the command again to assign the policy (with its associated slots or ports) to an existing power rule. For example:

-> lanpower power-policy NewPolicy power-rule NewRule

- When assigning a policy to a slot or port, be sure to use the syntax, “slot” or “port”, before the chassis/slot or chassis/slot/port values in the command line. Refer to the examples below for more information.

**Examples**

-> lanpower slot 1/1 power-policy NewPolicy
-> lanpower port 1/1/23 power-policy NewPolicy
-> lanpower power-policy NewPolicy power-rule NewRule
-> no lanpower port 1/1/23 power-policy
-> no lanpower power-policy NewPolicy

**Release History**

Release 8.1.1; command was introduced.
Release 8.7R2; port and slot options added for use with the no parameter.

**Related Commands**

- **lanpower power-rule**
  Specifies user-defined power rules that can be assigned to PoE ports.
- **show lanpower power-rule**
  Displays current PoE power rule settings.
- **show lanpower power-policy**
  Displays existing power policies assigned to a slot, port or rule.

**MIB Objects**

- **alaPethPowerPolicyTable**
  - **alaPethPowerPolicyRowStatus**
- **alaPethPowerPortTable**
  - **alaPethPowerPortPolicyName**
  - **alaPethPowerPortRowStatus**
**lanpower class-detection**

Enables or disables class detection of attached devices. When class detection is enabled, attached devices will automatically be limited to their class power, regardless of port power configuration.

```
lanpower {chassis chassis | slot chassis/slot} class-detection {enable | disable}
```

**Syntax Definitions**

- `chassis`  
  The chassis on which class detection is being enabled or disabled.
- `chassis/slot`  
  The particular slot on which class detection is being enabled or disabled.
- `enable`  
  Enables class detection on the specified slot.
- `disable`  
  Disables class detection on the specified slot.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Although class-detection is disabled by default, the OmniSwitch 6860 still provides power to incoming PDs (if available in the power budget). However, to strictly enforce class detection as specified in the 802.3at standard, class detection must be enabled using the `lanpower slot class-detection` command.
- Enabling class detection will reset all PoE ports on the chassis.

**Examples**

```
-> lanpower slot 1/1 class-detection enable
-> lanpower chassis 1 class-detection disable
```

**Release History**

- Release 8.1.1; command was introduced.
- Release 8.3.1; command was updated.
**Related Commands**

- `show lanpower class-detection` Displays class detection status on a specified slot.

**MIB Objects**

- `alaPethMainPseTable`
  - `alaPethMainPseClassDetection`
**lanpower capacitor-detection**

Enables or disables the capacitor detection method.

```
lanpower {chassis chassis | slot chassis/slot | port chassis/slot/port[-port]} capacitor-detection {enable | disable}
```

---

**Syntax Definitions**

- `chassis`: The chassis on which detection is being configured.
- `chassis/slot`: The slot on which detection is being configured.
- `chassis/slot/port-port`: The port or range of ports on which detection is being configured.
- `enable`: Enables the capacitor detection method on the specified slot.
- `disable`: Disables the capacitor detection method on the specified slot.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The capacitor detection method should only be enabled if there are legacy IP phones attached to the corresponding slot—this feature is not compatible with IEEE specifications. Please contact your Alcatel-Lucent Enterprise sales engineer or Customer Support representative to find out which Alcatel-Lucent Enterprise IP phones models need capacitive detection enabled.

---

**Examples**

```
-> lanpower slot 3/1 capacitor-detection enable
-> lanpower chassis 1 capacitor-detection disable
```

---

**Release History**

- Release 8.1.1; command was introduced.
- Release 8.3.1; command was updated.
- Release 8.8R1; `port` parameter added.
Related Commands

```
show lanpower capacitor-detection
```
Displays capacitor detection status on a specified slot.

MIB Objects

```
alaPethMainPseTable
  alaPethMainPseCapacitorDetect
```
**lanpower usage-threshold**

Tells the switch to watch for a user-defined, slot-wide threshold for PoE power usage, in percent. When the usage threshold is reached or exceeded, a notification is sent to the user.

```
lanpower {chassis chassis | slot chassis/slot} usage-threshold num
```

**Syntax Definitions**

- `chassis`: The chassis for which usage threshold monitoring is being set.
- `chassis/slot`: The slot for which usage threshold monitoring is being set.
- `num`: The percentage of allowed usage from attached PoE devices before a notification is sent to the user.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>num</code></td>
<td>99</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `lanpower slot usage-threshold` does not affect the amount of PoE power allocated to a particular slot. The command is a monitoring method that tells the switch to send a “specified usage exceeded” notification (i.e., trap) only when a specified percentage has been reached.

**Examples**

- `-> lanpower slot 1/1 usage-threshold 50`
- `-> lanpower chassis 1 usage-threshold 99`

**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.
Related Commands

show lanpower usage-threshold Displays current usage threshold, in percent.

MIB Objects

pethMainPseTable
  pethMainPseUsageThreshold
lanpower dynamic-power-mgmt

Enables dynamic power management for a chassis or slot.

```
lanpower {chassis chassis | slot chassis/slot} dynamic-power-management {enable | disable}
```

### Syntax Definitions

- **chassis**: The chassis on which dynamic power management is being enabled or disabled.
- **chassis/slot**: The particular slot on which dynamic power management is being enabled or disabled.
- **enable**: Enables dynamic power management on the specified chassis or slot.
- **disable**: Disables dynamic power management on the specified chassis or slot.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enabling this feature allows the unused allocated PoE power of an NI to be allocated to other NIs.
- Slot ranges are supported in the command line syntax.

### Examples

```
-> lanpower slot 1/1 dynamic-power-mgmt enable
-> lanpower chassis 1 dynamic-power-mgmt disable
```

### Release History

Release 8.3.1; command was introduced.

### MIB Objects

N/A
**lanpower update-from**

Updates the PoE microcontroller firmware.

```
lanpower update-from
```

### Syntax Definitions

- **chassis/slot**
  - The slot to be updated.

- **all**
  - Update all the chassis in a virtual chassis.

- **filename**
  - The file name of the PoE firmware.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The binary file must be placed in the `/flash` directory of the Master.
- Once started, console messages will be displayed during the update procedure which may take up to 10 minutes.
- The lanpower service must be disabled during the update and minimal load should be placed on the switch. The update process must be allowed to finish prior to unplugging or configuring the units.

### Examples

```
-> lanpower slot 1/1 update-from poe_binary_version.bin
```

### Release History

Release 8.1.1; command was introduced.
Related Commands

show lanpower firmware-upgrade-status Displays current PoE firmware update status.

MIB Objects

N/A
**lanpower 4pair**

Configures 2-pair or 4-pair PoE mode.

```
lanpower {slot chassis/slot | port chassis/slot/port-port} 4pair {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis/slot</td>
<td>The slot on which to configure the PoE mode.</td>
</tr>
<tr>
<td>chassis/slot/port-port</td>
<td>The port(s) on which to configure the PoE mode.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enabled</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360-P48X</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is applicable for 4-pair high power PoE ports to deliver 60 watts or more.
- When 4-pair mode is enabled the switch will consider Alt-A and Alt-B pairs for PoE.
- When 4-pair mode is disabled the switch will only consider Alt-A pairs for PoE.
- When 4-pair mode is disabled the maximum PoE power for the port is 30W.

### Examples

```
-> lanpower slot 1/1 4pair enable
```

### Release History

Release 8.4.1.R03; command was introduced.
Related Commands

show lanpower

Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

alaPethMainPseTable

alaPethPsePort4PairStatus
lanpower power-over-hdmi

Configures power over HDMI (PoH).

```
lanpower {slot chassis/slot | port chassis/slot/port-port} power-over-hdmi {enable | disable}
```

**Syntax Definitions**

- `chassis/slot` The slot on which to configure PoH.
- `chassis/slot/port-port` The port(s) on which to configure PoH.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6860(E) models do not support 802.3.bt. However, this command can be used to enable support for some products such as Aruba and Stellar APs with up to ~40W of PoE power.

**Examples**

```
-> lanpower slot 1/1 power-over-hdmi enable
-> lanpower port 1/1/1 power-over-hdmi enable
```

**Release History**

Release 8.6R2; command was introduced.
Related Commands

**show lanpower**

Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

alaPethPowerPortTable

alaPethPsePortPowerOverHdmi
**lanpower 802.3bt**

Enables IEEE 802.3bt functionality.

```
lanpower {slot chassis/slot | port chassis/slot/port} 802.3bt {enable | disable}
```

### Syntax Definitions

- `chassis/slot/port` The slot or port on which to enable or disable 802.3bt.
- `chassis/slot/port-port` The port(s) on which to enable or disable 802.3bt.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>C32E</td>
<td>C32E</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>C32C2</td>
<td>C32C2</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command can only be executed when the lanpower service is stopped.

### Examples

- `-> lanpower slot 1/1 802.3bt enable`
- `-> lanpower port 1/1/1 802.3bt enable`

### Release History

Release 8.6R2; command was introduced.

### Related Commands

- **show lanpower** Displays the PoE status and related statistics for all ports in a specified slot.

### MIB Objects

- `alaPethMainPseTable`
  - `alaPethMainPseDot3bt`
**lanpower fpoe**

Enables fast PoE functionality.

`lanpower {slot chassis/slot} fpoe {enable | disable}`

---

**Syntax Definitions**

- `chassis/slot`: The slot on which to enable or disable fast PoE.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Fast PoE can be used to provide PoE power within a few seconds after powering on the chassis.
- Factory default switches that don't have any PoE configuration must have an initial PoE configuration completed.
- The PoE configuration cannot be modified until the switch is up and the PoE module is completely initialized.
- LLDP-based PoE devices will not function as expected until the switch has completed its bootup and the switch is in a state to respond to LLDP requests.
- When Fast PoE is enabled the vcboot.cfg should not be deleted or manually edited.
- If Fast PoE is disabled all PDs will reset due to the PoE controller having to be reconfigured.
- FPGA/CPLD upgrade may be required. Refer to the release notes.

---

**Examples**

- `-> lanpower slot 1/1 fpoe enable`

---

**Release History**

Release 8.7R1; command was introduced.
**Related Commands**

*show lanpower*  
Displays the PoE status and related statistics for all ports in a specified slot.

**MIB Objects**

alaPethMainPseTable  
alaPethMainPseFastPoE
**lanpower ppoe**

Enables perpetual PoE functionality.

```
lanpower {slot chassis/slot} ppo {enable | disable}
```

### Syntax Definitions

`chassis/slot` The slot on which to enable or disable perpetual PoE.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This feature allows the switch to provide uninterrupted power to connected power device (PD) even when the switch is rebooting.
- When Perpetual PoE is enabled the vcboot.cfg should not be deleted or manually edited.
- FPGA/CPLD upgrade may be required. Refer to the release notes.

### Examples

```
-> lanpower slot 1/1 ppo enable
```

### Release History

Release 8.7R1; command was introduced.
Related Commands

*show lanpower*  Displays the PoE status and related statistics for all ports in a specified slot.

MIB Objects

*alaPethMainPseTable*

*alaPethMainPsePerpetualPoE*
**lanpower high-resistance-detection**

Configures high resistance detection.

```
lanpower {slot chassis/slot} high-resistance-detection {enable | disable}
```

### Syntax Definitions

- `chassis/slot`: The slot on which to enable or disable high resistance detection.

### Defaults

- `enable` or `disable`

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This capability can be enabled to support the two-port PoE capability on APs with two PoE ports (i.e. AP225). This capability enables the switch to support the appropriate detection range and recognize the AP as a PD.

- The AP will be powered in an active/standby mode, meaning only one port of the AP will be powered at a time.

- Only two-pair PoE will be supported when this feature is enabled, even on ports connected with a 4-pair Ethernet cable.

- The capability of PSE-to-PSE protection function is reduced when this feature is enabled. It is recommended to disable PoE on ports that do not have PDs connected.

- Enabling this feature will cause the PoE functionality to restart on the OmniSwitch. Additionally, this functionality does not follow the PoE IEEE standards.

### Examples

```
-> lanpower slot 1/1 high-resistance-detection enable
```

### Release History

Release 8.7R1; command was introduced.
Related Commands

*show lanpower high-resistance-detection* Displays the high resistance detection status.

MIB Objects

alaPethMainPseTable
- alaPethMainPseHighResistanceDetection
**lanpower trust**

Configures a port as trusted so that it can be powered down through 802.3bt LLDP tlv.

```bash
lanpower trust {slot chassis/slot| port chassis/slot/port-port} trust {enable | disable}
```

**Syntax Definitions**

- `chassis/slot`: The slot on which to enable or disable port trust.
- `chassis/slot/port-port`: The port(s) on which to enable or disable port trust.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In the 802.3BT LLDP standard the tlv has an option to power down the PSE port through LLDP for a specific time or indefinitely if the port is set as trusted.

**Examples**

```bash
-> lanpower port 1/1/1 trust enable
```

**Release History**

Release 8.7R1; command was introduced.

**Related Commands**

- **show lanpower**: Displays the PoE status and related statistics for all ports in a specified slot.

**MIB Objects**

- `alaPethPsePortTable`:
  - `alaPethPsePortTrusted`
show lanpower

Displays the PoE status and related statistics for all ports in a specified slot.

show lanpower {slot chassis/slot | port-config | chassis chassis port-config}

Syntax Definitions

chassis
The virtual chassis ID for which current inline power status and related statistics are to be displayed.

slot
The slot for which current inline power status and related statistics are to be displayed.

port-config
Displays detailed port configuration information and settings.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show lanpower slot 1/1

<table>
<thead>
<tr>
<th>Port</th>
<th>Maximum(mW)</th>
<th>Actual Used(mW)</th>
<th>Status</th>
<th>Priority</th>
<th>On/Off</th>
<th>Class</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>30000</td>
<td>7000</td>
<td>Powered On</td>
<td>Low</td>
<td>ON</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>1/1/2</td>
<td>30000</td>
<td>0</td>
<td>Powered Off</td>
<td>Low</td>
<td>OFF</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>1/1/3</td>
<td>30000</td>
<td>0</td>
<td>Powered Off</td>
<td>Low</td>
<td>OFF</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>1/1/4</td>
<td>30000</td>
<td>0</td>
<td>Powered Off</td>
<td>Low</td>
<td>OFF</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>1/1/5</td>
<td>30000</td>
<td>4100</td>
<td>Powered On</td>
<td>Low</td>
<td>ON</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>1/1/6</td>
<td>30000</td>
<td>0</td>
<td>Powered Off</td>
<td>Low</td>
<td>OFF</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>1/1/7</td>
<td>30000</td>
<td>0</td>
<td>Searching</td>
<td>Low</td>
<td>ON</td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>1/1/8</td>
<td>30000</td>
<td>0</td>
<td>Powered Off</td>
<td>Low</td>
<td>OFF</td>
<td></td>
<td>*</td>
</tr>
</tbody>
</table>

ChassisId 1 Slot 1 Max Watts 130
11 Watts Actual Power Consumed
119 Watts Actual Power Budget Remaining
130 Watts Total Power Budget Available
1 Power Supply Available

'*' appending port maxpower indicates 4pair port operating in 2pair modeBPS power:
### Power over Ethernet (PoE) Commands

#### show lanpower

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>A PoE port for which current status and related statistics are being displayed.</td>
</tr>
<tr>
<td>Maximum (mW)</td>
<td>The current maximum amount of power available to the corresponding PoE port, in milliwatts. For more information on this parameter, including default values and changing the settings, refer to the <a href="#">lanpower power</a> command.</td>
</tr>
<tr>
<td>Actual Used (mW)</td>
<td>The actual amount of power being used by an attached device (if applicable), in milliwatts. If no device is attached to the corresponding port, this row displays a value of 0.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the port's current operational status. Options include Powered On, Powered Off, Searching, Fault, Deny and Test. Powered On indicates that PoE power activation is complete and the attached device is receiving power. Powered Off indicates that no PoE device is attached and/or the port is not receiving PoE power. Searching indicates that PoE activation has started and a powered device PD has been detected, but activation or class detection is incomplete. Fault indicates that PoE activation or class detection has failed. Deny indicates that PoE power management has denied power to the port due to priority disconnect or over subscription. Test indicates that the port has been forced on and will remain on until it is forced off by RTP functions.</td>
</tr>
<tr>
<td>Priority</td>
<td>The current priority level for the corresponding PoE port. Options include Critical, High, and Low. Critical should be reserved for ports that have mission-critical devices attached, and therefore require top (i.e., critical) priority. In the event of a power management issue, inline power to critical ports is maintained as long as possible. High indicates ports that have important, but not mission-critical, devices attached. If other ports in the chassis have been configured as critical, inline power to high-priority ports is given second priority. Low priority is for ports that have low-priority devices attached. In the event of a power management issue, inline power to low-priority ports is interrupted first (i.e., before critical and high-priority ports). The default value is Low. Priority levels can be changed using the <a href="#">lanpower priority</a> command.</td>
</tr>
<tr>
<td>On/Off</td>
<td>Displays whether a port has been manually turned on or off by the user. ON indicates that the port has been turned on by the user via the <a href="#">lanpower service</a> command. OFF is the default value and can also indicate that the port has been turned off by the user via the <a href="#">lanpower service</a> command.</td>
</tr>
<tr>
<td>Class</td>
<td>PoE class detected on the attached Powered Device. See the <a href="#">lanpower class-detection</a> command on page 2-21 for more information.</td>
</tr>
<tr>
<td>Type</td>
<td>A user-defined name port type (i.e., text string) for the port. See the <a href="#">lanpower type</a> command on page 2-6 for more information.</td>
</tr>
<tr>
<td>Max Watts</td>
<td>The maximum watts available to the corresponding slot. The maximum watts value for a slot can be changed using the <a href="#">lanpower maxpower</a> command.</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actual Power Consumed</td>
<td>The amount of power being used by attached PoE devices.</td>
</tr>
<tr>
<td>Actual Power Budget Remaining</td>
<td>The amount of power budget remaining for PoE. If the total power budget remaining is exceeded, a power error will occur and the switch’s chassis management software will begin shutting down power to PoE ports according to their priority levels.</td>
</tr>
<tr>
<td>Total Power Budget Available</td>
<td>The total amount of power budget available for PoE.</td>
</tr>
<tr>
<td>Power Supplies Available</td>
<td>The number of power supplies currently installed and operating in the switch.</td>
</tr>
<tr>
<td>*</td>
<td>An asterisk indicates a 4-pair PoE port is operating in 2-pair mode.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.1.1; command was introduced.  
Release 8.8R1; `port-config` parameter added.

**Related Commands**

N/A

**MIB Objects**

- alaPethPsePortPowerActual  
- alaPethPsePortPowerMaximum  
- alaPethPsePortPowerStatus  
- pethPsePortPowerPriority  
- pethPsePortAdminEnable  
- pethPsePortPowerClass
show lanpower power-rule

Displays current PoE power rule settings.

show lanpower power-rule [name]

Syntax Definitions

name

The name of an existing power rule.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Entering the show lanpower power-rule command without the name string provides top-level information for all existing power rules. To view detailed information for a particular rule (e.g., timer and timezone settings, etc.), specify the name string in the command line.

Examples

-> show lanpower power-rule
Power-Rule                          Admin-state   Power
----------------------------------+------------+---------------------
test                                 Disabled      Off

-> show lanpower power-rule test
Power-Rule : test
Admin-state : Disabled
Power : Off
At HH:MM : 00:00
Day-of-Week : All
Month-of-Year : All
Timezone : Local

output definitions

| Power-Rule | The name(s) of existing PoE power rule(s). |
| Admin-state | The port PoE status assigned to the rule. Refer to page 2-16 for more information. |
**Output Definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>The PoE power status assigned to the rule. Refer to page 2-16 for more information.</td>
</tr>
<tr>
<td>At HH:MM</td>
<td>The time of day the power rule takes effect. Refer to page 2-16 for more information.</td>
</tr>
<tr>
<td>Day-of-Week</td>
<td>The day of the week the power rule takes effect. Refer to page 2-17 for more information.</td>
</tr>
<tr>
<td>Month-of-Year</td>
<td>The month of year the power rule takes effect. Refer to page 2-17 for more information.</td>
</tr>
<tr>
<td>Timezone</td>
<td>The timezone under which the power rule takes effect. Options include local-server, originator-server and utc. Refer to page 2-17 for more information.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

`lanpower power-rule` Specifies user-defined power rules that can be assigned to PoE ports.

**MIB Objects**

N/A
show lanpower power-policy

Displays existing power policies assigned to a slot, port or rule.

show lanpower power-policy [policy-name slot | policy-name power-rule | policy-name port]

Syntax Definitions

policy-name  The text string for an existing power policy.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/</th>
<th>6900V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Entering the show lanpower power-policy command without the policy-name string provides top-level information for all existing policies, including associated power rules (if any). To view detailed information for a particular policy, specify the policy-name string in the command line, along with the policy’s associated slot, port or rule. See Examples below for additional information.

Examples

-> show lanpower power-policy
  Power-Policy name                  Power-rules
  ----------------------------------+----------------------------------
  Mar25                              RuleTest2

-> show lanpower power-policy Mar25 power-rule
  Power-Policy name                  : Mar25
  Power-rules                        : RuleTest2

output definitions

<table>
<thead>
<tr>
<th>Power-Policy name</th>
<th>The names of existing PoE power policies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power-rules</td>
<td>The power rules associated with the existing power policies.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.
Related Commands

**lanpower power-policy**

Allows users to bind existing power rules to particular slots or ports.

MIB Objects

- N/A
show lanpower class-detection

Displays class detection status on a specified slot.

show lanpower {chassis chassis | slot chassis/slot } class-detection

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis for which class detection is being displayed.</td>
</tr>
<tr>
<td>chassis/slot</td>
<td>The slot for which class detection is being displayed.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Although class-detection is disabled by default, the OmniSwitch 6860 still provides power to incoming PDs (if available in the power budget). However, to strictly enforce class detection as specified in the 802.3at standard, class detection must be enabled using the lanpower slot class-detection command.

- Enabling class detection will reset all PoE ports on the chassis.

Examples

-> show lanpower slot 1/1 class-detection
Class Detection disabled on ChassisId 1 Slot 1

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower class-detection Enables or disables class detection of attached devices.

MIB Objects

N/A
show lanpower capacitor-detection

Displays capacitor detection status on a specified slot.

`show lanpower {chassis chassis | slot chassis/slot} capacitor-detection`

**Syntax Definitions**

- `chassis` The chassis for which capacitor detection is being displayed.
- `chassis/slot` The slot for which capacitor detection is being displayed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show lanpower slot 1/1 capacitor-detection
Capacitor Detection disabled on ChassisId 1 Slot 1
```

**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

**Related Commands**

- `lanpower capacitor-detection` Enables or disables the capacitor detection method.

**MIB Objects**

N/A
show lanpower priority-disconnect

Displays current priority disconnect status for a specified slot.

```bash
show lanpower {chassis chassis | slot chassis/slot} priority-disconnect
```

### Syntax Definitions

- **chassis**: The chassis on which priority disconnect status is being displayed.
- **chassis/slot**: The particular slot on which priority disconnect status is being displayed.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power (per power supply installed). For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power (per power supply installed).

### Examples

```bash
$ show lanpower slot 1/1 priority-disconnect
Priority Disconnect enabled on ChassisId 1 Slot 1
```

### Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

### Related Commands

- **lanpower priority-disconnect**: Enables or disables the priority disconnect function on all ports in a specified slot.

### MIB Objects

N/A
show lanpower ni-priority

Displays current Network Interface (NI) modules status for a specified chassis or slot.

show lanpower {chassis chassis | slot chassis/slot} ni-priority

Syntax Definitions

chassis          The chassis on which NI priority is being displayed.
chassis/slot     The particular slot on which NI priority is being displayed.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

For OmniSwitch 6860 switches using 920W power supplies, priority disconnect supports up to a maximum of 780W of PoE power (per power supply installed). For switches using 600W power supplies, priority disconnect supports up to a maximum of 450W of PoE power (per power supply installed).

Examples

-> show lanpower slot 1/1 priority-disconnect
Priority Disconnect enabled on ChassisId 1 Slot 1

Release History

Release 8.3.1; command was introduced.

Related Commands

lanpower ni-priority Specifies power priority level to a Network Interface (NI) module. Levels include critical, high, and low.

MIB Objects

N/A
show lanpower usage-threshold

Displays current usage threshold, in percent.

show lanpower {chassis chassis | slot chassis/slot} usage-threshold

Syntax Definitions

chassis
The chassis on which priority disconnect status is being displayed.

chassis/slot
The particular slot on which priority disconnect status is being displayed.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

```
-> show lanpower slot 1/1 usage-threshold
Usage Threshold 99% on ChassisId 1 Slot 1
```

Release History

Release 8.1.1; command was introduced.
Release 8.3.1; command was updated.

Related Commands

lanpower usage-threshold Sets a slot-wide threshold for PoE power usage, in percent.

MIB Objects

N/A
show lanpower firmware-upgrade-status

Displays the PoE firmware update status.

show lanpower slot \{chassis/slot | all\} firmware-upgrade-status

**Syntax Definitions**

- **chassis/slot**: Display the update status for a slot.
- **all**: Display the update status for all chassis.

**Defaults**

N/A

**Platforms Supported**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can be used to display the update progress from a remote session such as Telnet or SSH.

**Examples**

```
-> show lanpower slot all firmware-upgrade-status
Chas/Slot   FW-Upgrade Status  FW Upgrade %   FW Rev   Fail Reason
-----------------------------------------------+-----------------+--------+------------------------------
1/1         SUCCESS           0            352    FIRMWARE UPGRADED
```

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- **lanpower update-from**: Updates the PoE microcontroller firmware.

**MIB Objects**

N/A
show lanpower high-resistance-detection

Displays the high resistance detection configuration.

show lanpower slot chassis/slot high-resistance-detection

Syntax Definitions

chassis/slot

Display the status for a slot.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360 6465 6560 6570M 6860 6860N 6865 6900 6900 V72/C32 6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes  Yes  Yes  No  Yes  Yes  Yes  No  No  No  No  Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show lanpower slot 1/1 high-resistance-detection
Chas/Slot high-resistance-detection
-----------------------------
  1/1   enable

Release History

Release 8.7R1; command was introduced.

Related Commands

lanpower high-resistance-detection

This command is used to enable/disable high resistance detection.

MIB Objects

N/A
show lanpower status

Displays the running lanpower configuration.

show lanpower slot chassis/slot status

### Syntax Definitions

`chassis/slot`  
Display the status for a slot.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show lanpower slot 1/1 status
Chas/Slot Status  Init Status  8023BT Supported  Priority Disconnect  Capacitor Detection  FPoE  PPoE  F/W Rev
--------------------------------------------------------------------------------------------------------
  1/1   enable  initialized  enable  disable  disable  disable  enable  352
```

Not Available

### output definitions

- **Chas/Slot**: Chassis/slot.
- **Status**: The lanpower status.
- **Init Status**: The lanpower initialization status.
- **8023BT Supported**: 802.3bt support status.
- **Priority Disconnect**: Priority disconnect status.
- **Capacitor Detection**: Capacitor detection status.
- **FPoE**: Fast PoE status.
- **PPoE**: Perpetual PoE status.
- **F/W Rev**: Firmware revision.
**Release History**

Release 8.7R2; command was introduced.

**Related Commands**

- **show lanpower**
  
  Displays the PoE status and related statistics for all ports in a specified slot.

**MIB Objects**

- `alaPethMainPseAdminStatus`
- `alaPethMainPsePriorityDisconnect`
- `alaPethMainPseCapacitorDetect`
- `alaPethMainPseFastPoE`
- `alaPethMainPsePerptualPoE`
3 UDLD Commands

This chapter describes the CLI commands used to configure the UDLD (UniDirectional Link Detection) protocol. UDLD operates at Layer 2 in conjunction with IEEE 802.3 Layer 1 fault detection mechanism. It is a protocol used for detecting and disabling unidirectional Ethernet fiber or copper connections to avoid interface malfunctions, Spanning Tree loops, media faults, and so on. It operates in two main modes normal and aggressive.

The two basic mechanisms that UDLD follows are:

- Advertises port identity and learns about its neighbors. This information is maintained in a cache table.
- It sends continuous echo messages when fast notifications are required.

MIB information for the UDLD commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>ALCATEL-IND1-UDLD-MIB.mib</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>alcatelIND1UDLDMIB</td>
</tr>
</tbody>
</table>

A summary of available commands is listed here:

```
udld
udld port
udld mode
udld probe-timer
udld echo-wait-timer
clear udld statistics port
show udld configuration
show udld configuration port
show udld statistics port
show udld neighbor port
show udld status port
```

Configuration procedures for UDLD are explained in “Configuring UDLD,” *OmniSwitch AOS Release 8 Network Configuration Guide.*
udld

Globally enables or disables UDLD protocol on the switch.

`udld {enable | disable}`

### Syntax Definitions

- **enable**: Globally enables UDLD on the switch.
- **disable**: Globally disables UDLD on the switch.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
| Yes            | Yes            | Yes            | Yes            | Yes            | Yes            | Yes            | No             | Yes             | No             |
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
```

### Usage Guidelines

- Auto-negotiation should be disabled on both ends of the link for UDLD to operate properly.
- The port shutdown by this command can be reset by using the `interfaces admin` command.

### Examples

```
-> udld enable
-> udld disable
```

### Release History

Release 7.1.1; command introduced.
Related Commands

- **udld port** Enables or disables UDLD status on a specific port or a range of ports.
- **show udld configuration** Displays the global status of UDLD configuration.
- **show udld configuration port** Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

- **alaUdldGlobalStatus**
  - **alaUdldGlobalConfigUdldStatus**
**udld port**

Enables or disables UDLD status on a specific port or a range of ports.

`udld port chassis/slot/port[-port2] [enable | disable]`

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number.
- **enable**: Enables UDLD status on a port.
- **disable**: Disables UDLD status on a port.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>chassis</th>
<th>6250</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>7250</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Auto-negotiation should be disabled on both ends of the link for UDLD to operate properly.
- The UDLD protocol must be enabled before using this command.
- The UDLD protocol is supported on link aggregate member ports.

**Examples**

- `udld port 1/1/3 enable`
- `udld port 1/1/6-10 enable`
- `udld port 1/2/4 disable`

**Release History**

Release 7.1.1; command introduced.
Related Commands

**udld**
Globally enables or disabled UDLD protocol on the switch.

**show udld configuration port**
Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

alaUdldPortConfigTable
alaUdldPortConfigUdldStatus
**udld mode**

Configures the UDLD operational mode on a specific port, a range of ports, or all ports.

```
udld [port [chassis/slot/port[-port2]]] mode {normal | aggressive}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number.
- **normal**: Specifies UDLD operation in the normal mode.
- **aggressive**: Specifies UDLD operation in the aggressive mode.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>aggressive</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td>X48C6/T48C6</td>
<td>X48C4E/V48C8</td>
<td>C32E/T24C2</td>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The UDLD protocol must be enabled before using this command.
- In case of faulty cable connection, the port which is configured in normal mode of operation is considered to be in the shutdown state.

### Examples

```
-> udld mode aggressive
-> udld mode normal
-> udld port 1/1/3 mode aggressive
-> udld port 1/2/4 mode normal
-> udld port 1/2/9-18 mode aggressive
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- `udld`  
  Globally enables or disables UDLD protocol on the switch.

- `show udld configuration port`  
  Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

**MIB Objects**

- `alaUdldPortConfigTable`  
- `alaUdldPortConfigUdldMode`
**udld probe-timer**

Configures the probe-message advertisement timer on a specific port, a range of ports, or all ports. Probe messages are transmitted periodically after this timer expires.

```
udld [port [chassis/slot/port|-port2]] probe-timer seconds
no udld [port [chassis/slot/port|-port2]] probe-timer
```

### Syntax Definitions

- `chassis` The chassis identifier.
- `slot/port|-port2` The slot and port number.
- `seconds` The probe-message transmission interval, in seconds.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>15</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>feature</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to reset the probe-message timer to the default value. Note that it is not necessary to specify the probe-message interval to reset it.

- The UDLD protocol must be enabled before using this command.

- Configure probe-advertisement timer with values varying in a range of 12-18 seconds for better convergence time and to avoid burst of probe advertisements.

### Examples

```
-> udld probe-timer 20
-> udld port 1/1/3 probe-timer 16
-> udld port 1/1/8-21 probe-timer 18
-> no udld probe-timer
-> no udld port 1/1/3 probe-timer
```
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **udld**  
  Globally enables or disables UDLD protocol on the switch.

- **show udld configuration port**  
  Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

**MIB Objects**

- **alaUdldPortConfigTable**
  - **alaUdldPortConfigUdldProbeIntervalTimer**
**udld echo-wait-timer**

Configures the echo based detection timer on a specific port, a range of ports, or all the ports. This is known as link detection period.

```
udld [port [chassis/slot/port[-port2]]] echo-wait-timer seconds
no udld [port [chassis/slot/port[-port2]]] echo-wait-timer
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number.
- **seconds**: The echo based detection period, in seconds.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>8</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to reset the echo based detection timer to the default value. Note that it is not necessary to specify the echo based timer to reset it.
- The UDLD protocol must be enabled before using this command.
- An echo message is expected in reply from the neighbor within this time duration, otherwise, the port is considered as faulty.

### Examples

```
-> udld echo-wait-timer 9
-> udld port 1/1/5 echo-wait-timer 12
-> udld port 1/1/7-16 echo-wait-timer 12
-> no udld echo-wait-timer
-> no udld port 1/1/3 echo-wait-timer
```
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>udld</td>
<td>Globally enables or disables UDLD protocol on the switch.</td>
</tr>
<tr>
<td>show udld configuration port</td>
<td>Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.</td>
</tr>
</tbody>
</table>

**MIB Objects**

alaUdldPortConfigTable
  alaUdldPortConfigUdldDetectionPeriodTimer
**clear udld statistics port**

Clears the UDLD statistics for a specific port or for all the ports.

```
clear udld statistics [port chassis/slot/port]
```

### Syntax Definitions

- `chassis` The chassis identifier.
- `slot/port` The slot and port number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

| Platform          | Supported
|-------------------|-----------
| 6360              | Yes       |
| 6465              | Yes       |
| 6560              | Yes       |
| 6570M             | Yes       |
| 6860              | Yes       |
| 6860N             | Yes       |
| 6865              | Yes       |
| 6900              | No        |
| V72/C32           | Yes       |
| 6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2 | Yes |
| 9900              | No        |

### Usage Guidelines

If the slot/port option is not specified, UDLD statistics for the switch is cleared.

**Examples**

```
-> clear udld statistics port 1/1/4
-> clear udld statistics
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **udld** Globally enables or disables UDLD protocol on the switch.
- **show udld statistics port** Displays the UDLD statistics for a specific port.

**MIB Objects**

- `alaUdldGlobalClearStats`
show udlD configuration

Displays the global status of UDLD configuration.

show udlD configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show udlD configuration

Global UDLD Status : disabled,
Global UDLD Mode : normal,
Global UDLD Probe Timer (Sec) : 15,
Global UDLD Echo-Wait Timer (Sec) : 8
Global UDLD Status : Disabled

Output definitions

<table>
<thead>
<tr>
<th>Global UDLD Status</th>
<th>Indicates the UDLD status on the switch. Options include enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global UDLD Mode</td>
<td>Indicates the UDLD mode on the switch. Options include normal or aggressive.</td>
</tr>
<tr>
<td>Global UDLD Probe Timer (Sec)</td>
<td>A probe-message is expected after this time period.</td>
</tr>
<tr>
<td>Global UDLD Echo-Wait Timer (Sec)</td>
<td>The detection of neighbor is expected with in this time period.</td>
</tr>
<tr>
<td>Global UDLD Status</td>
<td>Indicates the UDLD status on the switch. Options include enabled or disabled.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **udld**
  Globally enables or disables UDLD protocol on the switch.

- **show udld configuration port**
  Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

**MIB Objects**

- **alaUdldGlobalStatus**
  - **alaUdldGlobalConfigUdldStatus**
show udlD configuration port

Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

show udlD configuration port [chassis/slot/port]

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number.

Defaults

By default, a list of all UDLD ports is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

```
-> show udlD configuration port
Slot/Port  Admin State  Oper Mode  Probe-Timer  Echo-Wait-Timer
-----------+---------------+------------+-------------+----------------
1/1/1      disabled       normal          15           10
1/1/2      disabled       normal          45           10
1/1/17     disabled       normal          33            8
1/1/18     disabled       normal          33            8
1/1/19     disabled       normal          33            8
1/1/20     disabled       aggressive       55            8
1/1/21     disabled       aggressive       55            8
1/1/22     disabled       aggressive       55            8
1/1/41     disabled       aggressive       77            8
1/1/42     enabled        aggressive       77            8
1/1/43     enabled        aggressive       77            8
1/1/44     enabled        aggressive       77            8
1/1/45     enabled        aggressive       77            8
```
-> show udld configuration port 1/1/1
Global UDLD Status : enabled,
Port UDLD Status   : enabled,
Port UDLD State    : bidirectional,
UDLD Op-Mode       : aggressive,
Probe Timer (Sec)  : 77,
Echo-Wait Timer (sec) : 8
output definitions

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Slot number for the module and physical port number on that module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDLD-State</td>
<td>Indicates the state of interface determined by UDLD operation, which can be notapplicable, shutdown, undetermined or bidirectional.</td>
</tr>
<tr>
<td>Oper-Mode</td>
<td>Indicates the operational mode of UDLD protocol. Options include normal or aggressive.</td>
</tr>
<tr>
<td>Global UDLD Status</td>
<td>Indicates the UDLD status on the switch. Options include enabled or disabled.</td>
</tr>
<tr>
<td>Port UDLD Status</td>
<td>Indicates the UDLD status on a port. Options include enable or disable.</td>
</tr>
<tr>
<td>Probe Timer</td>
<td>A probe-message is expected after this time period.</td>
</tr>
<tr>
<td>Echo-Wait Timer</td>
<td>The detection of neighbor is expected with in this time period.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

**udld mode**

Configures the operational mode of UDLD on a specific port, a range of ports, or all the ports.

**udld probe-timer**

Configures the probe-message advertisement timer on a specific port, a range of ports, or all the ports.

**udld echo-wait-timer**

Configures the echo based detection timer on a specific port, a range of ports, or all the ports.

MIB Objects

alaUdldGlobalStatus
alaUdldGlobalConfigUdldStatus
alaUdldPortConfigTable
alaUdldPortConfigUdldOperationalStatus
alaUdldPortConfigUdldMode
alaUdldPortConfigUdldStatus
alaUdldPortConfigUdldProbeintervalTimer
alaUdldPortConfigUdldDetectionPeriodTimer
alaUdldPortNeighborStatsTable
alaUdldNeighborName
show udld statistics port

Displays the UDLD statistics for a specific port.

show udld statistics port chassis/slot/port

Syntax Definitions

chassis                      The chassis identifier.
slot/port                    The slot and port number.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show udld statistics port 1/1/42

UDLD Port Statistics
Hello Packet Send      : 8,  
Echo Packet Send      : 8,  
Flush Packet Recvd    : 0  

UDLD Neighbor Statistics
Neighbor ID  HelloPktsRecv  EchoPktsRecv
-----------  ---------------  ---------------
1            8               15               
2            8               15               
3            8               21               
4            8               14               
5            8               15               
6            8               20               

output definitions

Hello Packet Send      The number of hello messages sent by a port.
Echo Packet Send      The number of echo messages sent by a port.
Flush Packet Recvd    The number of UDLD-Flush message received by a port.
output definitions (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor ID</td>
<td>The name of the neighbor.</td>
</tr>
<tr>
<td>Hello Pkts Recv</td>
<td>The number of hello messages received from the neighbor.</td>
</tr>
<tr>
<td>Echo Pkts Recv</td>
<td>The number of echo messages received from the neighbor.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

- **udld probe-timer**: Configures the probe-message advertisement timer on a specific port, a range of ports, or all the ports.
- **udld echo-wait-timer**: Configures the echo based detection timer on a specific port, a range of ports, or all the ports.

MIB Objects

alaUdldPortNeighborStatsTable
- alaUdldNeighborName
- alaUdldNumHelloSent
- alaUdldNumHelloRcvd
- alaUdldNumEchoSent
- alaUdldNumEchoRcvd
- alaUdldNumFlushRcvd
show udld neighbor port

Displays the UDLD neighbor ports.

show udld neighbor port chassis/slot/port

Syntax Definitions

chassis
The chassis identifier.

slot/port
The slot and port number.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show udld neighbor port 1/1/42

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Device Id</th>
<th>Port Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:d0:95:ea:b2:48</td>
<td>00:d0:95:ea:b2:78</td>
</tr>
<tr>
<td>2</td>
<td>00:d0:95:ea:b2:48</td>
<td>00:d0:95:ea:b2:79</td>
</tr>
<tr>
<td>3</td>
<td>00:d0:95:ea:b2:48</td>
<td>00:d0:95:ea:b2:74</td>
</tr>
<tr>
<td>4</td>
<td>00:d0:95:ea:b2:48</td>
<td>00:d0:95:ea:b2:75</td>
</tr>
<tr>
<td>5</td>
<td>00:d0:95:ea:b2:48</td>
<td>00:d0:95:ea:b2:76</td>
</tr>
<tr>
<td>6</td>
<td>00:d0:95:ea:b2:48</td>
<td>00:d0:95:ea:b2:77</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>The name of the neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device ID</td>
<td>The device ID.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port ID.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **udld echo-wait-timer**
  Configures the echo based detection timer on a specific port, a range of ports, or all the ports. This is known as link detection period.

- **show udld statistics port**
  Displays the UDLD statistics for a specific port.

**MIB Objects**

- `alaUdldPortNeighborStatsTable`
- `alaUdldNeighborName`
show udld status port

Displays the UDLD status for all ports or for a specific port.

**show udld status port [chassis/slot/port]**

### Syntax Definitions

- **chassis**
  - The chassis identifier.
- **slot/port**
  - The slot and port number.

### Defaults

By default, a list of all UDLD ports is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 C32E/T24C2/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X24C2</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

`-> show udld status port`

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Admin State</th>
<th>Operational State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>disabled</td>
<td>not applicable</td>
</tr>
<tr>
<td>1/1/2</td>
<td>disabled</td>
<td>not applicable</td>
</tr>
<tr>
<td>1/1/3</td>
<td>disabled</td>
<td>not applicable</td>
</tr>
<tr>
<td>1/1/21</td>
<td>disabled</td>
<td>not applicable</td>
</tr>
<tr>
<td>1/1/40</td>
<td>disabled</td>
<td>not applicable</td>
</tr>
<tr>
<td>1/1/41</td>
<td>disabled</td>
<td>not applicable</td>
</tr>
<tr>
<td>1/1/42</td>
<td>enabled</td>
<td>bidirectional</td>
</tr>
<tr>
<td>1/1/43</td>
<td>enabled</td>
<td>bidirectional</td>
</tr>
<tr>
<td>1/1/44</td>
<td>enabled</td>
<td>bidirectional</td>
</tr>
<tr>
<td>1/1/45</td>
<td>enabled</td>
<td>bidirectional</td>
</tr>
<tr>
<td>1/1/46</td>
<td>enabled</td>
<td>bidirectional</td>
</tr>
<tr>
<td>1/1/47</td>
<td>enabled</td>
<td>bidirectional</td>
</tr>
<tr>
<td>1/1/48</td>
<td>enabled</td>
<td>bidirectional</td>
</tr>
</tbody>
</table>

`-> show udld status port 1/1/44`

Admin State : enabled,
Operational State : bidirectional
show udld status port

output definitions

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Slot number for the module and physical port number on that module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Indicates whether UDLD is administratively enabled or disabled.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Indicates the state of interface determined by UDLD operation, which can be notapplicable, shutdown, undetermined or bidirectional.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

**udld port**
Enables or disables UDLD status on a specific port or a range of ports.

**show udld configuration port**
Displays the configuration information for all UDLD ports or for a particular UDLD port on the switch.

MIB Objects

alaUdldGlobalStatus
alaUdldPortConfigTable
  alaUdldPortConfigUdldOperationalStatus
4 Source Learning Commands

The Source Learning capability of OmniSwitch is responsible for creating, updating, and deleting source and destination MAC Address entries in the MAC Address Table. This chapter includes descriptions of Source Learning commands used to create or delete static MAC addresses, define the aging time value for static and dynamically learned MAC addresses, and display MAC Address Table entries and statistics.

MIB information for Source Learning commands is as follows:

Filename: ALCATEL-IND1-MAC-ADDRESS-MIB.mib
Module: alcatelIND1MacAddressMIB

A summary of the available commands is listed here:

mac-learning
mac-learning flush
domain all
mac-learning flush domain vlan
domain spb
mac-learning flush domain vxlan
domain l2gre
domain local
domain static mac-address
domain vlan static mac-address
domain spb static mac-address
domain vxlan static mac-address
domain local static mac-address
domain multicast mac-address
learning aging-time
learning mode
show mac-learning
domain all
domain vlan
domain spb
domain vxlan
domain l2gre
domain local
learning aging-time
learning-state
learning mode
mac-learning

Configures the status of source MAC address learning on a VLAN, a single port, a range of ports, or on a link aggregate of ports.

`mac-learning {vlan vlan[-vlan2] | port chassis/slot/port[-port2] | linkagg agg_id} {enable | disable}`

### Syntax Definitions

- `vlan[-vlan2]` The VLAN ID number. Use a hyphen to specify a range of VLAN IDs.
- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id` The link aggregate ID number.
- `enable` Enables source learning.
- `disable` Disables source learning.

### Defaults

By default, source learning is enabled on all ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Disabling source learning on a port or link aggregate is not supported on the OmniSwitch 6360, 6465, 6560, 6570M or 9900.
- Configuring source learning is not supported on Learned Port Security (LPS) and Universal Network Profile (UNP) ports, as well as individual ports that are members of a link aggregate.
- When port-based source learning is configured for a link aggregate ID, it affects all the ports that are members of the link aggregate.
- When source learning is disabled on a port or link aggregate, dynamic learning of MAC addresses is stopped.
- Static MAC addresses associated with a port or link aggregate are *not* cleared when source learning is disabled. Also, new static MAC address configurations are allowed on ports or link aggregates on which source learning is disabled.
Disabling source learning on a port or link aggregate is useful on a ring configuration, where switch A does not have to learn MAC addresses from switch B, or for a Transparent LAN Service, where service provider does not require the MAC addresses of the customer network.

**Examples**

-> mac-learning port 1/2 enable
-> mac-learning linkagg 10 disable
-> mac-learning vlan 10 disable

**Release History**

Release 7.1.1; command added.

**Related Commands**

- show mac-learning learning-state Displays the source learning status of a port or link aggregate on the switch.

**MIB Objects**

- slMacLearningVlanControlTable
  - slMacLearningVlanControlStatus
- slMacLearningControlTable
  - slMacLearningControlStatus
mac-learning flush

Clears the specified MAC addresses from the Source Learning MAC Address Table on the local switch.

```
mac-learning flush {dynamic | static | multicast} [mac-address mac_address]
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Clears dynamically learned MAC addresses.</td>
</tr>
<tr>
<td>static</td>
<td>Removes static MAC addresses.</td>
</tr>
<tr>
<td>multicast</td>
<td>Removes static multicast MAC addresses.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Enter the MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c).</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Release</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command flushes dynamically learned addresses from the MAC Address Table.
- Static unicast and static multicast addresses are removed. This command replaces the `no` form of the `mac-learning` command that was used in previous releases.

**Examples**

```
-> mac-learning flush dynamic
-> mac-learning flush dynamic mac-address 00:00:39:59:f1:0c
-> mac-learning flush static
-> mac-learning flush static mac-address 00:00:39:59:f1:0d
-> mac-learning flush multicast
-> mac-learning flush multicast mac-address 01:25:9a:5c:2f:10
```

**Release History**

Release 7.3.1; command added.
Related Commands

**show mac-learning**
Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

alaSlMacAddressGlobalTable
slMacAddressGblManagement
slMacAddressGblRowStatus
**mac-learning flush domain all**

Clears the specified MAC addresses from the Source Learning MAC Address Table for all learning domains on the local switch.

```
mac-learning flush domain all {dynamic | static}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Clears dynamically learned MAC addresses from all of the domains.</td>
</tr>
<tr>
<td>static</td>
<td>Removes static MAC addresses from all of the domains.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for all domains.
- Static unicast and static multicast addresses are removed.
- The `mac-learning flush` command replaces the `no` form of the `mac-learning` command that was used in previous releases.

### Examples

```
-> mac-learning flush domain all dynamic
-> mac-learning flush domain all static
```

### Release History

Release 7.3.1; command added.
Related Commands

- **mac-learning flush**
  Clears the MAC Address Table for the local switch.
- **mac-learning flush domain vlan**
  Clears MAC addresses from the VLAN learning domain.
- **mac-learning flush domain spb**
  Clears MAC addresses from the SPB learning domain.
- **mac-learning flush domain vxlan**
  Clears MAC addresses from the VXLAN learning domain.
- **mac-learning flush domain l2gre**
  Clears MAC addresses from the L2 GRE tunnel learning domain.
- **show mac-learning**
  Displays Source Learning MAC Address Table information for the local switch.

MIB Objects

- slMacAddressGblManagement
- slMacAddressGblRowStatus
**mac-learning flush domain vlan**

Clears the specified MAC addresses from the Source Learning MAC Address Table for the VLAN learning domain on the local switch.

```plaintext
mac-learning flush domain vlan {vlan vlan_id} {port chassis/slot/port | linkagg agg_id} | {dynamic | static | static-multicast} [mac-address mac_address]
```

**Syntax Definitions**

- `vlan_id`: VLAN ID number.
- `chassis`: The chassis identifier.
- `slot/port`: The slot and port number (3/1).
- `agg_id`: Enter a link aggregate ID number.
- `dynamic`: Clears dynamically learned MAC addresses from the VLAN domain.
- `static`: Removes static MAC addresses from the VLAN domain.
- `static-multicast`: Removes static multicast MAC addresses from the VLAN domain.
- `mac_address`: Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>all MAC addresses</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the VLAN domain.
- Static unicast and static multicast addresses are removed.
• The **static-multicast** parameter is *not* available for use with the following **mac-learning flush** commands:
  - **mac-learning flush domain all**
  - **mac-learning flush domain spb**
  - **mac-learning flush domain vxlan**
  - **mac-learning flush domain l2gre**
  - **mac-learning flush domain local**

• The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

**Examples**

```
-> mac-learning flush domain vlan vlan 20 port 1/2 dynamic
-> mac-learning flush domain vlan static
-> mac-learning flush domain vlan linkagg 10 static
```

**Release History**

Release 7.3.1; command added.

**Related Commands**

- **mac-learning flush**
  Clears the MAC Address Table for the local switch.

- **mac-learning flush domain spb**
  Clears MAC addresses from the SPB learning domain.

- **mac-learning flush domain vxlan**
  Clears MAC addresses from the VXLAN learning domain.

- **mac-learning flush domain l2gre**
  Clears MAC addresses from the L2 GRE tunnel learning domain.

- **show mac-learning**
  Displays Source Learning MAC Address Table information for the local switch.

**MIB Objects**

- **alaSlMacAddressGlobalTable**
- **slMacAddressGblManagement**
- **slMacAddressGblRowStatus**
mac-learning flush domain spb

Clears the specified MAC addresses from the Source Learning MAC Address Table for the Shortest Path Bridging (SPB) learning domain on the local switch.

```
mac-learning flush domain spb {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[:service_id] | isid instance_id} {dynamic | static} [mac-address mac_address]
```

**Syntax Definitions**

- **service_id**
  - An existing SPB service ID.
- **chassis**
  - The chassis identifier.
- **slot/port:encap**
  - The SPB access port and encapsulation (0, all, qtag, or outer_qtag.inner_qtag) for an SPB Service Access Point (SAP).
- **sdp_id[:service_id]**
  - Clears MAC addresses learned on an SPB Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are cleared.
- **instance_id**
  - An SPB backbone service instance identifier (I-SID).
- **dynamic**
  - Clears dynamically learned MAC addresses from the SPB domain.
- **static**
  - Removes static MAC addresses from the SPB domain.
- **mac_address**
  - Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>all MAC addresses</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the SPB domain.
- Static unicast and static multicast addresses are removed.
The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

### Examples

- `-> mac-learning flush domain spb dynamic`
- `-> mac-learning flush domain spb sap 1/12:0 dynamic`
- `-> mac-learning flush domain spb serviceid 10 isid 1500 dynamic`

### Release History

Release 7.3.1; command added.

### Related Commands

- **mac-learning flush** 
  Clears the MAC Address Table for the local switch.
- **mac-learning flush domain vlan** 
  Clears MAC addresses from the VLAN learning domain.
- **mac-learning flush domain vxlan** 
  Clears MAC addresses from the VXLAN learning domain.
- **mac-learning flush domain l2gre** 
  Clears MAC addresses from the L2 GRE tunnel learning domain.
- **show mac-learning** 
  Displays Source Learning MAC Address Table information for the local switch.

### MIB Objects

- `alaSlMacAddressGlobalTable`
- `slMacAddressGblManagement`
- `slSvcISID`
- `slMacAddressGblRowStatus`
mac-learning flush domain vxlan

Clears the specified MAC addresses from the Source Learning MAC Address Table for the Virtual eXtensible LAN (VXLAN) learning domain on the local switch.

```
mac-learning flush domain vxlan {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[:service_id] | vnid vxlan_id} {dynamic | static} [mac-address mac_address]
```

**Syntax Definitions**

- **service_id**: An existing VXLAN service ID.
- **chassis**: The chassis identifier.
- **slot/port:encap**: The VXLAN access port and encapsulation (0, all, qtag, or outer_qtag,inner_qtag) for a VXLAN Service Access Point (SAP).
- **sdp_id[:service_id]**: Clears MAC addresses learned on a VXLAN Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
- **vxlan_id**: A 24-bit numerical value that identifies a VXLAN segment (a VXLAN network ID). The valid range is 1–2147483647 (or 000.000.001–255.255.255 in decimal notation format). Use a hyphen to specify a range of IDs (25001-25005).
- **dynamic**: Clears dynamically learned MAC addresses from the VXLAN domain.
- **static**: Removes static MAC addresses from the VXLAN domain.
- **mac_address**: Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>all MAC addresses</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the VXLAN domain.
• Static unicast and static multicast addresses are removed.

• The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

**Examples**

```
-> mac-learning flush domain vxlan dynamic
-> mac-learning flush domain vxlan sap 1/12:0 dynamic
-> mac-learning flush domain vxlan serviceid 10 vnid 23000 dynamic
```

**Release History**

Release 7.3.4; command added.

**Related Commands**

- **mac-learning flush** Clear the MAC Address Table for the local switch.
- **mac-learning flush domain vlan** Clear MAC addresses from the VLAN learning domain.
- **mac-learning flush domain spb** Clear MAC addresses from the SPB learning domain.
- **mac-learning flush domain l2gre** Clear MAC addresses from the L2 GRE tunnel learning domain.
- **show mac-learning** Displays Source Learning MAC Address Table information for the local switch.

**MIB Objects**

- `alaSlMacAddressGlobalTable`
  - `slMacAddressGblManagement`
  - `slVxLanVnID`
  - `slMacAddressGblRowStatus`
mac-learning flush domain l2gre

Clears the specified MAC addresses from the Source Learning MAC Address Table for the Layer 2 Generic Routing Encapsulation (L2 GRE) learning domain on the local switch.

Syntax

```
mac-learning flush domain l2gre {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[:service_id] | vpnid vpn_id} {dynamic | static} [mac-address mac_address]
```

Syntax Definitions

- **service_id**: An existing L2 GRE service ID.
- **chassis**: The chassis identifier.
- **slot/port:encap**: The access port and encapsulation (0, all, qtag, or outer_qtag.inner_qtag) for an L2 GRE Service Access Point (SAP).
- **sdp_id[:service_id]**: Clears MAC addresses learned on an L2 GRE Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
- **vpnid**: A tunnel ID that identifies a GRE tunnel VPN.
- **dynamic**: Clears dynamically learned MAC addresses from the L2 GRE domain.
- **static**: Removes static MAC addresses from the L2 GRE domain.
- **mac_address**: Enter a specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>all MAC addresses</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the L2 GRE tunnel domain.
- Static unicast and static multicast addresses are removed.
- The **mac-learning flush** command replaces the **no** form of the **mac-learning** command that was used in previous releases.

**Examples**

-> mac-learning flush domain l2gre dynamic
-> mac-learning flush domain l2gre sap 1/1/12:0 dynamic
-> mac-learning flush domain l2gre serviceid 10 vpnid 200 dynamic

**Release History**

Release 8.4.1.R02; command introduced.

**Related Commands**

- **mac-learning flush**
  - Clears the MAC Address Table for the local switch.
- **mac-learning flush domain vlan**
  - Clears MAC addresses from the VLAN learning domain.
- **mac-learning flush domain spb**
  - Clears MAC addresses from the SPB learning domain.
- **mac-learning flush domain vxlan**
  - Clears MAC addresses from the VXLAN learning domain.
- **show mac-learning**
  - Displays Source Learning MAC Address Table information for the local switch.

**MIB Objects**

- `alaSlMacAddressGlobalTable`
- `slMacAddressGblManagement`
- `slL2GreVpnID`
- `slMacAddressGblRowStatus`
mac-learning flush domain local

Clears the specified MAC addresses from the Source Learning MAC address table for the local service learning domain.

`mac-learning flush domain local serviceid service_id [sap chassis/slot/port:encap] static [mac-address mac_address]`

**Syntax Definitions**

- `service_id` – An existing service ID.
- `chassis` – The chassis identifier.
- `slot/port:encap` – The service access port and encapsulation (0, all, qtag, or outer_qtag.inner_qtag) for a Service Access Point (SAP).
- `mac_address` – Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>all MAC addresses</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>support</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command flushes dynamically learned addresses from the MAC Address Table that were learned or statically configured for the service domain.
- Static unicast and static multicast addresses are removed.
- The `mac-learning flush` command replaces the `no` form of the `mac-learning` command that was used in previous releases.

**Examples**

- `-> mac-learning flush domain local serviceid 10 static`
- `-> mac-learning flush domain local serviceid 20 sap 1/1/13:20 static`

**Release History**

Release 7.3.1; command added.
Related Commands

- **`mac-learning flush`**: Clears the MAC Address Table for the local switch.
- **`mac-learning flush domain vlan`**: Clears MAC addresses from the VLAN learning domain.
- **`mac-learning flush domain spb`**: Clears MAC addresses from the Shortest Path Bridging (SPB) learning domain.
- **`mac-learning flush domain vxlan`**: Clears MAC addresses from the Virtual eXtensible LAN (VXLAN) learning domain.
- **`show mac-learning`**: Displays Source Learning MAC address table information for the local switch.

MIB Objects

- `alaSlMacAddressGlobalTable`:
  - `slMacDomain`
  - `slLocaleType`
  - `slOriginId`
  - `slServiceId`
  - `slSubId`
  - `slMacAddressGb1`
  - `slMacAddressGb1Management`
  - `slMacAddressGb1Disposition`
  - `slMacAddressGb1RowStatus`
  - `slMacAddressGb1Protocol`
  - `slMacAddressGb1GroupField`
**mac-learning static mac-address**

Configures a static destination unicast MAC address. The configured MAC address is assigned to a fixed switch port or link aggregate ID and VLAN. If the destination of the data packets received on the VLAN ports is the configured MAC address, then they are forwarded to the specific MAC address port.

```
mac-learning {vlan vlan_id [port chassis/slot/port | linkagg agg_id]} static mac-address mac_address [bridging | filtering]
```

```
mac-learning flush [vlan vlan_id [port chassis/slot/port | linkagg agg_id]] static [mac-address mac_address]
```

### Syntax Definitions

- `vlan_id`: VLAN ID number.
- `chassis`: The chassis identifier.
- `slot/port`: The slot and port number (3/1) that is assigned to the static MAC address.
- `agg_id`: Enter a link aggregate ID number. See Chapter 12, “Link Aggregation Commands.”
- `mac_address`: Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
- `bridging`: Specifies that all packets to or from this MAC address are bridged.
- `filtering`: Specifies that all packets to or from this MAC address are filtered or dropped.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging, filtering</td>
<td>bridging</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `mac-learning flush` command to remove a static MAC address from the Source Learning MAC Address Table. Note that if no parameters are specified with this command, then all static addresses are removed.

- Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address port.
• Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.

• The destination MAC addresses are maintained in the Source Learning MAC address table.

• If a packet received on a port associated with the same VLAN contains a source address that matches a static MAC address, then the packet is discarded.

**Examples**

- `mac-learning vlan 10 port 1/10 static mac-address 00:00:39:59:f1:0c bridging`
- `mac-learning vlan 20 linkagg 5 static mac-address 00:00:9a:55:e0:01 filtering`
- `mac-learning flush vlan 500 static`
- `mac-learning flush vlan 10 port 1/10 static mac-address 00:00:39:59:f1:0c`
- `mac-learning flush vlan 20 linkagg 5 static`
- `mac-learning flush static`

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1: `mac-learning flush` command replaced the `no mac-learning` command.

**Related Commands**

- `vlan members untagged` Assigns ports and link aggregates to a VLAN.
- `mac-learning multicast mac-address` Configures a static multicast MAC address and assigns the address to one or more egress ports or link aggregates.
- `show mac-learning` Displays Source Learning MAC Address Table information.

**MIB Objects**

- `alaSlMacAddressGlobalTable`  
  `slOriginId`  
  `slServiceId`  
  `slMacAddressGbl`  
  `slMacAddressGblManagement`  
  `slMacAddressGblDisposition`
mac-learning domain vlan static mac-address

Configures a static destination unicast MAC address in the VLAN source learning domain. The configured MAC address is assigned to a fixed switch port or link aggregate ID and VLAN. If the destination of the data packets received on the VLAN ports is the configured static MAC address, then they are forwarded to the specific MAC address port.

```
mac-learning domain vlan vlan vlan_id [port chassis/slot/port | linkagg agg_id] static mac-address mac_address [bridging | filtering]
```

```
mac-learning flush domain vlan [vlan vlan_id [port chassis/slot/port | linkagg agg_id]] static [mac-address mac_address]
```

**Syntax Definitions**

- **vlan_id**: VLAN ID number.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1) that is assigned to the static MAC address.
- **agg_id**: Enter a link aggregate ID number. See Chapter 12, “Link Aggregation Commands.”
- **mac_address**: Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
- **bridging**: Specifies that all packets to or from this MAC address are bridged.
- **filtering**: Specifies that all packets to or from this MAC address are filtered or dropped.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging</td>
<td>bridging</td>
</tr>
<tr>
<td>filtering</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `mac-learning flush` command to remove a static MAC address from the Source Learning MAC Address Table. Note that if no parameters are specified with this command, then all static addresses are removed.
• Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address port.

• Select the filtering parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the bridging parameter for regular traffic flow to or from the MAC address.

• The destination MAC addresses are maintained in the Source Learning MAC address table.

• If a packet received on a port associated with the same VLAN contains a source address that matches a static MAC address, then the packet is discarded.

**Examples**

```
-> mac-learning domain vlan vlan 10 port 1/1/10 static mac-address 00:00:39:59:f1:0c bridging
-> mac-learning domain vlan vlan 20 linkagg 5 static mac-address 00:00:9a:55:e0:01 filtering
-> mac-learning flush domain vlan vlan 500 static
-> mac-learning flush domain vlan vlan 10 port 1/1/10 static mac-address 00:00:39:59:f1:0c
-> mac-learning flush domain vlan vlan 20 linkagg 5 static
-> mac-learning flush domain vlan static
```

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1: **mac-learning flush** command replaced the **no mac-learning** command.

**Related Commands**

- **vlan members untagged** Assigns ports and link aggregates to a VLAN.
- **mac-learning flush domain vlan** Clears MAC addresses from the VLAN source learning domain.
- **show mac-learning** Displays Source Learning MAC Address Table information.

**MIB Objects**

- **alaSlMacAddressGlobalTable**
  - **slMacDomain**
  - **slOriginId**
  - **slServiceId**
  - **slMacAddressGb1**
  - **slMacAddressGb1Management**
  - **slMacAddressGb1Disposition**
  - **slMacAddressGb1RowStatus**
mac-learning domain spb static mac-address

Configures a static destination unicast MAC address in the Shortest Path Bridging (SPB) source learning domain.

```
mac-learning domain spb {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id:service_id} static mac-address mac_address [bridging | filtering]
```

```
mac-learning domain spb {instance_id |.sap chassis/slot/port:encap | bind-sdp sdp_id:service_id} static mac-address mac_address [bridging | filtering]
```

```
mac-learning flush domain spb {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id:service_id | isid instance_id} static [mac-address mac_address]
```

### Syntax Definitions

- **service_id**: An existing SPB service ID.
- **instance_id**: An SPB backbone service instance identifier (I-SID).
- **chassis**: The chassis identifier.
- **slot/port:encap**: The SPB access port and encapsulation (0, qtag, or outer_qtag.inner_qtag) for an SPB Service Access Point (SAP).
- **sdp_id:service_id**: The SPB Service Distribution Point (SDP) ID number and service ID number for a specific binding.
- **mac_address**: Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
- **bridging**: Specifies that all packets to or from this MAC address are bridged.
- **filtering**: Specifies that all packets to or from this MAC address are filtered or dropped.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging</td>
<td>bridging</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **mac-learning flush** command to remove a static MAC address from the Source Learning MAC Address Table. Note that if no parameters are specified with this command, then all static addresses are removed.
• Select the **filtering** parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the **bridging** parameter for regular traffic flow to or from the MAC address.

• The destination MAC addresses are maintained in the Source Learning MAC address table.

• If a packet received on an access port associated with the same SAP contains a source address that matches a static MAC address, then the packet is discarded.

**Examples**

```
-> mac-learning domain spb serviceid 10 sap 1/1/12:0 static mac-address 00:00:39:59:f1:0c bridging
-> mac-learning domain spb isid 1500 sap 1/1/12:0 static mac-address 00:00:39:59:f1:0c filtering
-> mac-learning flush domain spb static
-> mac-learning flush domain spb sap 1/1/12:0 static mac-address 00:00:39:59:f1:0c
-> mac-learning flush domain spb serviceid 10 isid 1500 static
```

**Release History**

Release 7.3.1; command added.

**Related Commands**

- `mac-learning flush domain spb` Clears MAC addresses from the SPB source learning domain.
- `mac-learning domain vlan static mac-address` Configures static MAC addresses in the VLAN source learning domain.
- `mac-learning domain vxlan static mac-address` Configures static MAC addresses in the Virtual eXtensible LAN (VXLAN) source learning domain.
- `show mac-learning domain spb` Displays MAC Address Table information for the SPB source learning domain.

**MIB Objects**

- `alaSlMacAddressGlobalTable`
  - `slMacDomain`
  - `slLocaleType`
  - `slOriginId`
  - `slServiceId`
  - `slSubId`
  - `slMacAddressGbl`
  - `slMacAddressGblManagement`
  - `slMacAddressGblDisposition`
  - `slMacAddressGblRowStatus`
  - `slMacAddressGblProtocol`
  - `slMacAddressGblGroupField`
  - `slSvcISID`
mac-learning domain vxlan static mac-address

Configures a static destination unicast MAC address in the Virtual eXtensible LAN (VXLAN) source learning domain

mac-learning domain vxlan {serviceid service_id [sap chassis/slot/port:encap | vnid vxlan_id [sap chassis/slot/port:encap]]} static mac-address mac_address [bridging | filtering]

mac-learning domain vxlan vnid vxlan_id sap chassis/slot/port:encap static mac-address mac_address [bridging | filtering]

mac-learning flush domain vxlan {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[:service_id] | vnid vxlan_id} static [mac-address mac_address]

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_id</td>
<td>An existing VXLAN service ID.</td>
</tr>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port:encap</td>
<td>The VXLAN access port and encapsulation (qtag, or outer_qtag.inner_qtag) for a VXLAN Service Access Point (SAP).</td>
</tr>
<tr>
<td>vxlan_id</td>
<td>A 24-bit numerical value that identifies an existing VXLAN segment (a VXLAN network ID).</td>
</tr>
<tr>
<td>mac_address</td>
<td>Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).</td>
</tr>
<tr>
<td>bridging</td>
<td>Specifies that all packets to or from this MAC address are bridged.</td>
</tr>
<tr>
<td>filtering</td>
<td>Specifies that all packets to or from this MAC address are filtered or dropped.</td>
</tr>
<tr>
<td>sdp_id[:service_id]</td>
<td>Use this parameter with the mac-learning flush command to specify a VXLAN Service Distribution Point (SDP) ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are cleared.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging</td>
<td>bridging</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- Use the `mac-learning flush` command to remove a static MAC address from the Source Learning MAC address table. Note that if no parameters are specified with this command, then all static addresses are removed.

- Select the `filtering` parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the `bridging` parameter for regular traffic flow to or from the MAC address.

- The destination MAC addresses are maintained in the Source Learning MAC address table.

- If a packet received on an access port associated with the same SAP contains a source address that matches a static MAC address, then the packet is discarded.

**Examples**

```plaintext
-> mac-learning domain vxlan serviceid 10 sap 1/1/12:10 static mac-address 00:00:39:59:f1:0c bridging
-> mac-learning domain vxlan vnil 23000 sap 1/1/12:10 static mac-address 00:00:39:59:f1:0c filtering
-> mac-learning flush domain vxlan static
-> mac-learning flush domain vxlan sap 1/12:0 static
-> mac-learning flush domain vxlan serviceid 10 vnil 23000 static
```

**Release History**

Release 7.3.4; command added.

**Related Commands**

- **mac-learning flush domain vxlan** Clears MAC addresses from the VXLAN source learning domain.
- **mac-learning domain vlan static mac-address** Configures static MAC addresses in the VLAN source learning domain.
- **mac-learning domain spb static mac-address** Configures static MAC addresses in the Shortest Path Bridging (SPB) source learning domain.
- **show mac-learning domain vxlan** Displays MAC Address Table information for the VXLAN source learning domain.

**MIB Objects**

- `alaSlMacAddressGlobalTable`
  - `slMacDomain`
  - `slLocaleType`
  - `slOriginId`
  - `slServiceId`
  - `slSubId`
  - `slMacAddressGbl`
  - `slMacAddressGblManagement`
  - `slMacAddressGblDisposition`
  - `slMacAddressGblRowStatus`
  - `slMacAddressGblProtocol`
  - `slMacAddressGblGroupField`
  - `slVxLanVnId`
**mac-learning domain local static mac-address**

Configures a static destination unicast MAC address for a local service in the source learning domain

```
mac-learning domain local serviceid service_id sap chassis/slot/port:encap static mac-address
mac_address [bridging | filtering]
```

```
mac-learning flush domain local serviceid service_id [sap chassis/slot/port:encap] static [mac-address mac_address]
```

### Syntax Definitions

- `service_id`: An existing service ID.
- `chassis`: The chassis identifier.
- `slot/port:encap`: The service access port and encapsulation (`qtag`, or `outer_qtag.inner_qtag`) for a VXLAN Service Access Point (SAP).
- `mac_address`: Enter a destination MAC Address (for example, 00:00:39:59:f1:0c).
- `bridging`: Specifies that all packets to or from this MAC address are bridged.
- `filtering`: Specifies that all packets to or from this MAC address are filtered or dropped.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridging</td>
<td>bridging</td>
</tr>
<tr>
<td>filtering</td>
<td>bridging</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

- Use the `mac-learning flush` command to remove a static MAC address from the Source Learning MAC address table. Note that if no parameters are specified with this command, then all static addresses are removed.
- Select the `filtering` parameter to set up a denial of service to block potential hostile attacks. Traffic sent to or from a filtered MAC address is dropped. Select the `bridging` parameter for regular traffic flow to or from the MAC address.
- The destination MAC addresses are maintained in the Source Learning MAC address table.
• If a packet received on an access port associated with the same SAP contains a source address that matches a static MAC address, then the packet is discarded.

**Examples**

```
-> mac-learning domain local serviceid 10 sap 1/1/12:10 static mac-address 00:00:39:59:f1:0c bridging
-> mac-learning domain local serviceid 20 sap 1/1/13:20 static mac-address 00:00:39:59:f1:0c filtering
-> mac-learning flush domain local serviceid 10 static
-> mac-learning flush domain local serviceid 20 sap 1/1/13:20 static
```

**Release History**

Release 7.3.1; command added.

**Related Commands**

- `mac-learning flush domain vxlan`
  - Clears MAC addresses from the VXLAN source learning domain.

- `mac-learning domain vlan static mac-address`
  - Configures static MAC addresses in the VLAN source learning domain.

- `mac-learning domain spb static mac-address`
  - Configures static MAC addresses in the Shortest Path Bridging (SPB) source learning domain.

- `mac-learning domain vxlan static mac-address`
  - Configures static MAC addresses in the Virtual eXtensible LAN (VXLAN) source learning domain.

- `show mac-learning domain local`
  - Displays MAC Address Table information for the Local source learning domain.

**MIB Objects**

- `alaS1MacAddressGlobalTable`
- `s1MacDomain`
- `s1LocaleType`
- `s1ServiceId`
- `s1OriginId`
- `s1SubId`
- `s1MacAddressGb1`
- `s1MacAddressGb1Management`
- `s1MacAddressGb1Disposition`
- `s1MacAddressGb1RowStatus`
- `s1MacAddressGb1Protocol`
- `s1MacAddressGb1GroupField`
mac-learning multicast mac-address

Configures a static multicast MAC address and assigns the address to one or more egress ports. Packets received on ports associated with the specified VLAN that contain a destination MAC address that matches the static multicast address are forwarded to the specified egress ports. Static multicast MAC addresses are maintained in the Source Learning MAC address table.

```
mac-learning {vlan vlan_id {port chassis/slot/port | linkagg agg_id }} multicast mac-address multicast_address [group group_id]
```

```
mac-learning flush {vlan vlan_id [port chassis/slot/port | linkagg agg_id ]] multicast [mac-address multicast_address]
```

**Syntax Definitions**

- `vlan_id` VLAN ID number.
- `chassis` The chassis identifier.
- `slot/port` The egress slot and port number (3/1) that is assigned to the static multicast MAC address.
- `agg_id` Enter a link aggregate ID number. See Chapter 12, "Link Aggregation Commands."
- `multicast_address` Enter the destination multicast MAC Address to add to the MAC Address Table (for example, 01:00:39:59:f1:0c).
- `group_id` This keyword cannot be user defined.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `mac-learning flush` command to remove a static multicast MAC address from the Source Learning MAC Address Table. Note that If no parameters are specified with this command, then all static multicast addresses are removed.
- Note that a MAC address is considered a multicast MAC address if the least significant bit of the most significant octet of the address is enabled. For example, MAC addresses with a prefix of 01, 03, 05, 13, and so on, are multicast MAC addresses.
If a multicast prefix value is not present, then the address is treated as a regular MAC address and not allowed when using the `mac-learning vlan multicast mac-address` command. Also note that multicast addresses within the following ranges are not supported:

01:00:5E:00:00:00 to 01:00:5E:7F:FF
01:80:C2:XX.XX.XX
33:33:XX:XX:XX

The configured (static) multicast MAC address is assigned to a fixed switch port or link aggregate ID and VLAN.

In addition to configuring the same static multicast address for multiple ports within a given VLAN, it is also possible to use the same multicast address across multiple VLANs.

Enter a port number or link aggregate ID that is already associated with the specified VLAN ID. Only traffic from other ports associated with the same VLAN is directed to the static MAC address port.

If the `configuration snapshot` or `write memory` command is entered after a static multicast MAC address is configured, the resulting ASCII file or `boot.cfg` file includes the “`group group_id`” as the additional syntax for the `mac-learning static-multicast` command. The “`group group_id`” indicates the number of the multicast group that the switch has assigned to the multicast MAC address for the given VLAN association. Each multicast address – VLAN association is treated as a unique instance and assigned a group number specific to that instance.

Note that if the port assigned to a multicast MAC address is down or administratively disabled when the `configuration snapshot` or `write memory` command is used, the multicast MAC address is not saved to the resulting ASCII file or `boot.cfg` file.

**Examples**

```
-> mac-learning vlan 1500 port 1/10 multicast mac-address 01:25:9a:5c:2f:10
-> mac-learning vlan 355 port 4/2-10 multicast mac-address 01:25:9a:5c:2f:11
-> mac-learning vlan 455 linkagg 10 multicast mac-address 01:25:9a:5c:2f:12
-> mac-learning flush vlan 500 multicast
-> mac-learning flush vlan 1500 port 1/10 multicast mac-address 01:25:9a:5c:2f:10
-> mac-learning flush vlan 455 linkagg 10 multicast mac-address 01:25:9a:5c:2f:12
-> mac-learning flush multicast
```

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; `mac-learning flush` command replaced the `no mac-learning` command.

**Related Commands**

- `vlan members untagged`: Assigns ports and link aggregates to a VLAN.
- `mac-learning static mac-address`: Configures a static MAC address and assigns the address to a port or link aggregate.
- `show mac-learning`: Displays Source Learning MAC Address Table information.

**MIB Objects**

- `alaSlMacAddressGlobalTable`
- `slOriginId`
- `slServiceId`
slMacAddressGbl
slMacAddressGblManagement
slMacAddressGblDisposition
mac-learning aging-time

Configures aging time, in seconds, for static and dynamically learned MAC addresses. When a MAC address has aged beyond the aging-time value, the MAC address is discarded.

**Command Syntax**

```plaintext
mac-learning aging-time {seconds | default}
no mac-learning aging-time
```

**Syntax Definitions**

- **seconds**: Aging time value (in seconds). Do not use commas in value.
- **default**: The aging time is set to the default value of 300 seconds.

**Defaults**

By default, the aging time is set to 300 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **default** parameter to set the aging-time back to the default value of 300 seconds.
- The aging time value is a global value that applies to all VLANs. Configuring this value on a per VLAN basis is not supported.
- Note that an inactive MAC address can take up to twice as long as the aging time value specified to be removed from the MAC address table. For example, if an aging time of 60 seconds is specified, the MAC address ages out any time between 60 and 120 seconds of inactivity.
- When a new MAC aging time is set, the aging process could take up to 3 aging cycles to age out the inactive macs. This only applies to the first time the aging time is set. Subsequent aging processes can take up to twice as long as the aging time value as described above.
- The MAC address table aging time is also used as the timeout value for the Address Resolution Protocol (ARP) table. This timeout value determines how long the switch retains dynamically learned ARP table entries.

**Examples**

```
-> mac-learning aging-time 1200
-> mac-learning aging-time default
```
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show mac-learning` Displays Source Learning MAC Address Table information.
- `show mac-learning aging-time` Displays the current aging time value for the Source Learning MAC Address Table.

**MIB Objects**

- `slMacAddressAgingTable`
- `slMacAgingValue`
mac-learning mode

Specifies the source learning mode for the chassis.

mac-learning mode [centralized | distributed]

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>centralized</td>
<td>Enables centralized MAC source learning mode.</td>
</tr>
<tr>
<td>distributed</td>
<td>Enables distributed MAC source learning mode.</td>
</tr>
</tbody>
</table>

Defaults

By default, centralized MAC source learning mode is enabled for the chassis.

Platforms Supported

Not supported in this release.

Usage Guidelines

After the distributed MAC mode is either enabled or disabled using this command, immediately save the switch configuration using the write memory command and then reboot the switch.

Examples

- `-> mac-learning mode centralized`
- `-> mac-learning mode distributed`

Release History

Release 7.1.1; command introduced.

Related Commands

`show mac-learning mode` Displays the current status of the MAC source learning mode.

MIB Objects

<table>
<thead>
<tr>
<th>Object ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slDistributedMacMode</td>
<td></td>
</tr>
</tbody>
</table>
show mac-learning

Displays Source Learning MAC Address Table information for the switch.

**Syntax**

```
show mac-learning [summary | dynamic | static | multicast | bmac] [port chassis/slot/port] [linkagg agg_id] [mac-address mac_address] [remote [mac-address mac_address]]
```

**Syntax Definitions**

- **summary**: Displays a summary of all the MAC address information.
- **dynamic**: Displays only dynamically learned MAC addresses.
- **static**: Displays only static MAC addresses with a permanent status.
- **multicast**: Displays only multicast MAC addresses.
- **bmac**: Displays only backbone MAC addresses (BMACs). A BMAC is the bridge MAC address of a Shortest Path Bridging (SPB) switch.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1).
- **agg_id**: The link aggregate ID number.
- **mac_address**: A MAC Address (for example, 00:00:39:59:f1:0c).

**Defaults**

By default, information is displayed for all MAC addresses contained in the table.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the `show mac-learning` command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.

- If there is a duplicate static MAC address occurrence, a “&” will appear to the right of the address in the `show mac-learning` command display.
Examples

-> show mac-learning summary
Mac Address Table Summary:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Static</th>
<th>Static-Multicast</th>
<th>Bmac</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>SPB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>LOCAL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VXLAN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>L2GRE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Total MAC Address In Use = 34

-> show mac-learning
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 10 e8:e7:32:11:d4:78</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/1/14</td>
</tr>
<tr>
<td>VLAN 52 e8:e7:32:42:e0:4d</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/3</td>
</tr>
<tr>
<td>VLAN 60 e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/4</td>
</tr>
<tr>
<td>VLAN 60 e8:e7:32:00:24:a5</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN 60 e8:e7:32:00:24:b3</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN 60 e8:e7:32:6c:5c:de</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/92</td>
</tr>
<tr>
<td>VLAN 100 e8:e7:32:42:e0:4d</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/98</td>
</tr>
<tr>
<td>VLAN 108 e8:e7:32:42:d8:6d</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/16</td>
</tr>
<tr>
<td>VLAN 208 e8:e7:32:42:e0:dd</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/15</td>
</tr>
<tr>
<td>VLAN 1000 e8:e7:32:00:27:e1</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/1/14</td>
</tr>
<tr>
<td>VLAN 1000 e8:e7:32:00:27:ee</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/1/14</td>
</tr>
<tr>
<td>VLAN 4000 e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/4</td>
</tr>
<tr>
<td>VLAN 4000 e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/4</td>
</tr>
<tr>
<td>VLAN 4000 e8:e7:32:00:24:a5</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN 4000 e8:e7:32:6c:5c:de</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/91</td>
</tr>
<tr>
<td>VLAN 4051 e8:e7:32:00:27:e1</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/4</td>
</tr>
<tr>
<td>VLAN 4051 e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/4</td>
</tr>
<tr>
<td>VLAN 4051 e8:e7:32:00:24:a5</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN 4051 e8:e7:32:6c:5c:de</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/91</td>
</tr>
<tr>
<td>VLAN 4052 e8:e7:32:00:27:e1</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/4</td>
</tr>
<tr>
<td>VLAN 4052 e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>1/5/4</td>
</tr>
<tr>
<td>VLAN 4052 e8:e7:32:00:24:a5</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN 4052 e8:e7:32:6c:5c:de</td>
<td>dynamic</td>
<td>bridging</td>
<td></td>
<td>0/91</td>
</tr>
<tr>
<td>SPB   1000:1000 e8:e7:32:11:db:72</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/1000</td>
<td>1/13/1000</td>
</tr>
<tr>
<td>SPB   1000:1000 e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:32867:1000</td>
<td></td>
</tr>
<tr>
<td>SPB   1000:1000 e8:e7:32:00:27:e1</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:32904:1000</td>
<td></td>
</tr>
<tr>
<td>SPB   1000:1000 e8:e7:32:00:27:ee</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:32904:1000</td>
<td></td>
</tr>
<tr>
<td>SPB   3899:3899 e8:e7:32:42:e0:4d</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/99:99</td>
<td></td>
</tr>
<tr>
<td>SPB   3899:3899 e8:e7:32:42:e0:5c</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/99:99</td>
<td></td>
</tr>
<tr>
<td>VXLAN 5:5 00:0e:1e:06:87:8c</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/1/20A</td>
<td></td>
</tr>
<tr>
<td>VXLAN 5:5 00:0c:0d:10:2c:cl</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/1/20A</td>
<td></td>
</tr>
<tr>
<td>VXLAN 5:5 00:0e:1e:0c:58:94</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:175:5</td>
<td></td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 34
-> show mac-learning bmac

Legend: Mac Address: * = address not valid,
       Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain</th>
<th>Vlan/SrvclId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>4000 e8:e7:32:00:27:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4000 e8:e7:32:40:10:7e</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4000 e8:e7:32:6c:5c:de</td>
<td>bmac</td>
<td>bridging</td>
<td>0/1</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>0/1</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>0/91</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>0/1</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:20:02:7:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>0/91</td>
<td></td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 12

output definitions

- **Domain**: The domain in which the MAC address was learned or statically configured (VLAN, SPB, VXLAN, L2GRE).

- **Vlan/SrvclId/[ISId/vnID]**: This field contains one of the following values depending on the domain type associated with the MAC address:
  - The VLAN ID number.
  - The SPB or VXLAN service ID number.
  - The ISID number associated with the SPB service ID number.
  - The VXLAN Network ID (VNID) number associated with the VXLAN service ID.
  - The GRE tunnel VPN ID number associated with the L2 GRE tunnel service ID.

- **Mac Address**: MAC address that is currently learned or statically assigned.

- **Type**: MAC address management status (dynamic, static, bmac).

- **Operation**: The disposition of the MAC address (bridging, filtering, servicing, quarantined).

- **Interface**: The slot/port number that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29). In the service domain, the Service Access Point (SAP) or the Service Distribution Point (SDP) associated with the MAC address is displayed.

**Release History**

- Release 7.1.1; command introduced.
- Release 7.3.1; show command display modified to include domain and service information.
- Release 7.3.4; vnID field added.
Related Commands

- **show mac-learning domain vlan**  Displays MAC Address Table information for the VLAN source learning domain.
- **show mac-learning domain spb**  Displays MAC Address Table information for the Shortest Path Bridging (SPB source learning domain.
- **show mac-learning domain vxlan**  Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
- **show mac-learning domain l2gre**  Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
- **show mac-learning aging-time**  Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

- **alaSlMacAddressGlobalTable**
  - slMacDomain
  - slLocaleType
  - slOriginId
  - slServiceId
  - slSubId
  - slMacAddressGbl
  - slMacAddressGblManagement
  - slMacAddressGblDisposition
  - slMacAddressGblRowStatus
  - slMacAddressGblGroupField
  - slSvcISID
  - slVxLanVnID
  - slL2GreVpnID
show mac-learning domain all

Displays MAC Address Table information for all source learning domains.

show mac-learning domain all [summary]

Syntax Definitions

summary Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.

- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

-> show mac-learning domain all summary
Mac Address Table Summary:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Static</th>
<th>Static-Multicast</th>
<th>Bmac</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>VPLS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>SPB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LOCAL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>VXLAN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>L2GRE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Total MAC Address In Use = 16
source Learning Commands

-> show mac-learning domain all
Legend: Mac Address: * = address not valid,
       & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 1</td>
<td>e8:e7:32:e4:0d:95</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/29B</td>
</tr>
<tr>
<td>VLAN 1</td>
<td>e8:e7:32:e4:0d:96</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/29C</td>
</tr>
<tr>
<td>VLAN 1</td>
<td>e8:e7:32:e4:0d:97</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/29D</td>
</tr>
<tr>
<td>VLAN 1</td>
<td>e8:e7:32:40:0b:9e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN 46</td>
<td>e8:e7:32:36:1e:f6</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN 46</td>
<td>e8:e7:32:40:0b:9e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN 71</td>
<td>00:0e:1e:06:87:88</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/20B</td>
</tr>
<tr>
<td>VLAN 1024</td>
<td>00:e0:b1:e7:17:a5</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/25</td>
</tr>
<tr>
<td>VLAN 1024</td>
<td>e8:e7:32:26:b6:0e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/25</td>
</tr>
<tr>
<td>VLAN 1026</td>
<td>00:e0:b1:db:c3:f1</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN 1026</td>
<td>e8:e7:32:40:0b:9e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VXLAN 5:5</td>
<td>00:0e:1e:06:87:8c</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:1/1/20A</td>
</tr>
<tr>
<td>VXLAN 5:5</td>
<td>00:c0:dd:10:2c:c1</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:1/1/20A</td>
</tr>
<tr>
<td>VXLAN 5:5</td>
<td>00:0e:1e:0c:58:94</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:175:5</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 16

**output definitions**

**Domain**
The domain in which the MAC address was learned or statically configured (VLAN, SPB, VXLAN, L2GRE).

**Vlan/SrvcId/[ISId/vnID]**
This field contains one of the following values depending on the domain type associated with the MAC address:
- The VLAN ID number.
- The SPB or VXLAN service ID number.
- The ISID number associated with the SPB service ID number.
- The VXLAN Network ID (VNID) number associated with the VXLAN service ID.
- The GRE tunnel VPN ID number associated with the L2 GRE tunnel service ID.

**Mac Address**
MAC address that is currently learned or statically assigned.

**Type**
MAC address management status (dynamic, static, bmac).

**Operation**
The disposition of the MAC address (bridging, filtering, servicing, quarantined).

**Interface**
The slot/port number that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29). In the service domain, the Service Access Point (SAP) or the Service Distribution Point (SDP) associated with the MAC address is displayed.

**Release History**
Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain information.
Release 7.3.4; vnID field added.
Source Learning Commands

show mac-learning
Displays Source Learning MAC Address Table information for the switch.

show mac-learning domain vlan
Displays MAC Address Table information for the VLAN source learning domain.

show mac-learning domain spb
Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.

show mac-learning domain vxlan
Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.

show mac-learning domain l2gre
Displays MAC Address Table information for the L2 GRE tunnel source learning domain.

show mac-learning aging-time
Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

alaSlMacAddressGlobalTable
  slMacDomain
  slOriginId
  slMacAddressGb1
  slMacAddressGb1Management
  slMacAddressGb1Disposition
  slMacAddressGb1RowStatus
  slMacAddressGb1GroupField
show mac-learning domain vlan

Displays MAC Address Table information for the VLAN source learning domain.

show mac-learning domain vlan [vlan vlan_id] [port chassis/slot/port | linkagg agg_id] [dynamic | static | static-multicast | bmac] [mac-address mac_address] [summary]

Syntax Definitions

- **vlan_id**: VLAN ID number.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1) that is assigned to the static MAC address.
- **agg_id**: A link aggregate ID number.
- **dynamic**: Displays dynamically learned MAC addresses.
- **static**: Displays static MAC addresses with a permanent status.
- **static-multicast**: Displays static multicast MAC addresses. This parameter applies only to the VLAN domain.
- **bmac**: Displays backbone MAC addresses (BMACs). A BMAC is the bridge MAC address of a SPB switch. This parameter applies only to the VLAN domain.
- **mac_address**: A MAC Address (for example, 00:00:39:59:f1:0c).
- **summary**: Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned for the VLAN domain are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.

- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.
Examples

-> show mac-learning domain vlan summary
Mac Address Table Summary:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Static</th>
<th>Static-Multicast</th>
<th>Bmac</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>17</td>
</tr>
</tbody>
</table>

Total MAC Address In Use = 29

-> show mac-learning domain vlan
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain VlanSrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>71 00:0f:e1:06:87:88</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/20B</td>
</tr>
<tr>
<td>VLAN</td>
<td>71 00:c0:dd:10:2c:c0</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/20B</td>
</tr>
<tr>
<td>VLAN</td>
<td>e8:e7:32:e4:0d:95</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/29B</td>
</tr>
<tr>
<td>VLAN</td>
<td>e8:e7:32:e4:0d:96</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/29C</td>
</tr>
<tr>
<td>VLAN</td>
<td>e8:e7:32:e4:0d:97</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/29D</td>
</tr>
<tr>
<td>VLAN</td>
<td>00:00:c9:e3:al:5f</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>e8:e7:32:40:0b:9e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>46 e8:e7:32:36:1e:fe</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>46 e8:e7:32:40:0b:9e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>312 00:00:5e:00:01:d4</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>312 00:e0:b1:db:c3:f1</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>312 e8:e7:32:26:b6:0e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>312 00:0e:00:00:01:d5</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>313 00:e0:bl:db:c3:f1</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>313 e8:e7:32:26:b6:0e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>313 e8:e7:32:40:0b:9e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 17

-> show mac-learning domain vlan vlan 312
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain VlanSrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>312 00:00:5e:00:01:d4</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>312 00:e0:bl:db:c3:f1</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>312 e8:e7:32:26:b6:0e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
<tr>
<td>VLAN</td>
<td>312 e8:e7:32:40:0b:9e</td>
<td>dynamic</td>
<td>bridging</td>
<td>0/24</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 4
-> show mac-learning domain vlan port 1/1/20
Legend: Mac Address: * = address not valid,
  Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>71 00:e6:1e:06:87:88</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/20</td>
</tr>
<tr>
<td>VLAN</td>
<td>71 00:c0:dd:10:2c:c0</td>
<td>dynamic</td>
<td>bridging</td>
<td>1/1/20</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 2

-> show mac-learning domain vlan bmac
Legend: Mac Address: * = address not valid,
  Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>4000 e8:e7:32:00:27:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
</tr>
<tr>
<td>VLAN</td>
<td>4000 e8:e7:32:40:10:7e</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
</tr>
<tr>
<td>VLAN</td>
<td>4000 e8:e7:32:00:24:a5</td>
<td>bmac</td>
<td>bridging</td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN</td>
<td>4000 e8:e7:32:6c:5c:de</td>
<td>bmac</td>
<td>bridging</td>
<td>0/91</td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:00:27:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:40:10:7e</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:00:24:a5</td>
<td>bmac</td>
<td>bridging</td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN</td>
<td>4051 e8:e7:32:6c:5c:de</td>
<td>bmac</td>
<td>bridging</td>
<td>0/91</td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:00:27:e1</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:40:10:7e</td>
<td>bmac</td>
<td>bridging</td>
<td>1/5/14</td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:00:24:a5</td>
<td>bmac</td>
<td>bridging</td>
<td>0/1</td>
</tr>
<tr>
<td>VLAN</td>
<td>4052 e8:e7:32:6c:5c:de</td>
<td>bmac</td>
<td>bridging</td>
<td>0/91</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 12

output definitions

<table>
<thead>
<tr>
<th>Domain</th>
<th>The domain in which the MAC address was learned or statically configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan/SrvcId/[ISId/vnID]</td>
<td>The VLAN ID number associated with the MAC address.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>MAC address that is currently learned or statically assigned.</td>
</tr>
<tr>
<td>Type</td>
<td>MAC address management status (dynamic, static, bmac).</td>
</tr>
<tr>
<td>Operation</td>
<td>The disposition of the MAC address (bridging, filtering, servicing, quarantined).</td>
</tr>
<tr>
<td>Interface</td>
<td>The slot/port number that is associated with the static or dynamically learned MAC address. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29).</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain information.
Related Commands

show mac-learning          Displays Source Learning MAC Address Table information for the switch.
show mac-learning domain spb Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
show mac-learning domain vxlan Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
show mac-learning domain l2gre Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
show mac-learning aging-time Displays the current aging time value for the Source Learning MAC Address Table.

MIB Objects

alaSlMacAddressGlobalTable
  slMacDomain
  slOriginId
  slMacAddressGbl
  slMacAddressGblManagement
  slMacAddressGblDisposition
  slMacAddressGblRowStatus
  slMacAddressGblGroupField
show mac-learning domain spb

Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.

```
show mac-learning domain spb [isid instance_id | serviceid service_id [isid instance_id]] [sap chassis/slot/port:encap | bind-sdp sdp_id[:service_id]] [dynamic | static] [mac-address mac_address] [summary]
```

**Syntax Definitions**

- **instance_id**: A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network. The valid range is 256–16777214.
- **service_id**: An existing SPB service ID.
- **chassis/slot/port:encap**: The SPB access port and encapsulation (all, qtag, or outer_qtag.inner_qtag) for an SPB Service Access Point (SAP). For example, 1/1/2:10.
- **mesh_id**: A SPB service distribution point (SDP) ID.
- **sdp_id[:service_id]**: Displays MAC addresses learned on an SPB Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
- **dynamic**: Displays dynamically learned MAC addresses.
- **static**: Displays static MAC addresses with a permanent status.
- **mac_address**: A MAC Address (for example, 00:00:39:59:f1:0c).
- **summary**: Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

**Defaults**

By default, all MAC address entries learned for the SPB domain are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC...
address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.

- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

**Examples**

```
-> show mac-learning domain spb summary
Mac Address Table Summary:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Static</th>
<th>Static-Multicast</th>
<th>Bmac</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPB</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>

Total MAC Address In Use = 6
```

```
-> show mac-learning domain spb
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPB</td>
<td>1000:1000</td>
<td>e8:e7:32:11:db:72</td>
<td>dynamic</td>
<td>servicing sap:1/1/13:1000</td>
</tr>
<tr>
<td>SPB</td>
<td>1000:1000</td>
<td>e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>servicing sdp:32867:1000</td>
</tr>
<tr>
<td>SPB</td>
<td>1000:1000</td>
<td>e8:e7:32:00:27:e1</td>
<td>dynamic</td>
<td>servicing sdp:32904:1000</td>
</tr>
<tr>
<td>SPB</td>
<td>1000:1000</td>
<td>e8:e7:32:00:27:ee</td>
<td>dynamic</td>
<td>servicing sdp:32904:1000</td>
</tr>
<tr>
<td>SPB</td>
<td>3899:3899</td>
<td>e8:e7:32:42:e0:4d</td>
<td>dynamic</td>
<td>servicing sap:0/99:99</td>
</tr>
<tr>
<td>SPB</td>
<td>3899:3899</td>
<td>e8:e7:32:42:e0:5c</td>
<td>dynamic</td>
<td>servicing sap:0/99:99</td>
</tr>
</tbody>
</table>
```

Total number of Valid MAC addresses above = 6

```
-> show mac-learning domain spb serviceid 3899
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPB</td>
<td>3899:3899</td>
<td>e8:e7:32:42:e0:4d</td>
<td>dynamic</td>
<td>servicing sap:0/99:99</td>
</tr>
<tr>
<td>SPB</td>
<td>3899:3899</td>
<td>e8:e7:32:42:e0:5c</td>
<td>dynamic</td>
<td>servicing sap:0/99:99</td>
</tr>
</tbody>
</table>
```

Total number of Valid MAC addresses above = 2

**output definitions**

- **Domain**: The domain in which the MAC address was learned or statically configured.
- **Vlan/SrvcId/[ISId/vnID]**: The SPB service ID number and the ISID number associated with the SPB service ID.
- **Mac Address**: MAC address that is currently learned or statically assigned.
- **Type**: MAC address management status (dynamic, static, bmac).
**output definitions**

<table>
<thead>
<tr>
<th>Operation</th>
<th>The disposition of the MAC address (bridging, filtering, servicing, quarantined).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The SPB service access point (SAP) associated with the MAC address.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain and service information.

**Related Commands**

- **show mac-learning**
  Displays Source Learning MAC Address Table information for the switch.

- **show mac-learning domain vlan**
  Displays MAC Address Table information for the VLAN source learning domain.

- **show mac-learning domain vxlan**
  Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.

- **show mac-learning domain l2gre**
  Displays MAC Address Table information for the L2 GRE tunnel source learning domain.

- **show mac-learning aging-time**
  Displays the current aging time value for the Source Learning MAC Address Table.

**MIB Objects**

alaSlMacAddressGlobalTable
- slMacDomain
- slLocaleType
- slOriginId
- slServiceId
- slSubId
- slMacAddressGbl
- slMacAddressGblManagement
- slMacAddressGblDisposition
- slMacAddressGblRowStatus
- slMacAddressGblGroupField
- slSvcISID
**show mac-learning domain vxlan**

Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.

```
show mac-learning domain vxlan [vnid vxlan_id | serviceid service_id [vnid vxlan_id]] [sap chassis/slot/port:encap | bind-sdp sdp_id[:service_id]] [dynamic | static] [mac-address mac_address] [summary]
```

### Syntax Definitions

- **vxlan_id**: A 24-bit numerical value that identifies a VXLAN segment (a VXLAN network ID). The valid range is 1–2147483647 (or 000.000.001–255.255.255 in decimal notation format). Use a hyphen to specify a range of IDs (25001-25005).

- **service_id**: An existing VXLAN service ID.

- **chassis(slot/port:encap**: The VXLAN service access port and encapsulation (0, all, qtag, or outer_qtag.inner_qtag) for a VXLAN Service Access Point (SAP). For example, 1/1/2:10.

- **sdp_id[:service_id]**: Displays MAC addresses learned on a VXLAN Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.

- **dynamic**: Displays dynamically learned MAC addresses.

- **static**: Displays static MAC addresses with a permanent status.

- **mac_address**: A MAC Address (for example, 00:00:39:59:f1:0c).

- **summary**: Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

### Defaults

By default, all MAC address entries learned for the VXLAN domain are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC...
address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.

- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

Examples

-> show mac-learning domain vxlan summary
Mac Address Table Summary:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Static</th>
<th>Static-Multicast</th>
<th>Bmac</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>VXLAN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

Total MAC Address In Use = 4

-> show mac-learning domain vxlan
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VXLAN</td>
<td>5:5 00:0e:1e:06:87:8c</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:1/1/20A</td>
</tr>
<tr>
<td>VXLAN</td>
<td>5:5 00:c0:dd:10:2c:c1</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:1/1/20A</td>
</tr>
<tr>
<td>VXLAN</td>
<td>5:5 00:0e:1e:0c:58:94</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:175:5</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 4

-> show mac-learning domain vxlan vnid 5 bind-sdp 175
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>VXLAN</td>
<td>5:5 00:0e:1e:0c:58:94</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:175:5</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 2

output definitions

- **Domain**: The domain in which the MAC address was learned or statically configured.
- **Vlan/SrvcId/[ISId/vnID]**: The VXLAN service ID number and VXLAN Network ID (VNID) number associated with the VXLAN service ID.
- **Mac Address**: MAC address that is currently learned or statically assigned.
- **Type**: MAC address management status (**dynamic**, **static**, **bmac**).
**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `show mac-learning` Displays Source Learning MAC Address Table information for the switch.
- `show mac-learning domain vlan` Displays MAC Address Table information for the VLAN source learning domain.
- `show mac-learning domain spb` Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
- `show mac-learning domain l2gre` Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
- `show mac-learning aging-time` Displays the current aging time value for the Source Learning MAC Address Table.

**MIB Objects**

- `alaSlMacAddressGlobalTable`
  - `slMacDomain`
  - `slLocaleType`
  - `slOriginId`
  - `slServiceId`
  - `slSubId`
  - `slMacAddressGbl`
  - `slMacAddressGblManagement`
  - `slMacAddressGblDisposition`
  - `slMacAddressGblRowStatus`
  - `slMacAddressGblGroupField`
  - `slVxLanVnID`
show mac-learning domain l2gre

Displays MAC Address Table information for the Layer 2 Generic Routing Encapsulation (L2 GRE) source learning domain.

show mac-learning domain l2gre {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[:service_id] | vpnid vpn_id} {dynamic | static} [mac-address mac_address] [summary]

Syntax Definitions

service_id An existing L2 GRE service ID.
chassis The chassis identifier.
slot/port:encap The access port and encapsulation (0, all, qtag, or outer_qtag.inner_qtag) for an L2 GRE Service Access Point (SAP).
sdp_id[:service_id] Displays MAC addresses learned on an L2 GRE Service Distribution Point (SDP) binding. Specify the SDP ID number and service ID number for a specific binding. If the optional service ID is not specified, MAC addresses learned for all bindings associated with the SDP ID are displayed.
vpnid A tunnel ID that identifies a GRE tunnel VPN.
dynamic Displays dynamically learned MAC addresses from the specified domain.
static Displays static MAC addresses from the specified domain.
mac_address A specific MAC Address to clear from the MAC Address Table (for example, 00:00:39:59:f1:0c) for the specified domain.
summary Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

Defaults

By default, all MAC address entries learned in the L2 GRE tunnel domain are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
• If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

**Examples**

```bash
-> show mac-learning domain l2gre summary
Mac Address Table Summary:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Static</th>
<th>Static-Multicast</th>
<th>Bmac</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2GRE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

Total MAC Address In Use = 4

-> show mac-learning domain l2gre
Legend: Mac Address: * = address not valid,
        Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2GRE</td>
<td>00:0e:1e:06:87:8c</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:1/1/20A</td>
</tr>
<tr>
<td>L2GRE</td>
<td>00:c0:dd:10:2c:c1</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:1/1/20A</td>
</tr>
<tr>
<td>L2GRE</td>
<td>00:0e:0e:0c:58:94</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:175:5</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 4

-> show mac-learning domain l2gre vpnid 5 bind-sdp 175
Legend: Mac Address: * = address not valid,
        Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2GRE</td>
<td>00:0e:1e:0c:58:94</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:175:5</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 2

**output definitions**

<table>
<thead>
<tr>
<th>Domain</th>
<th>Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
</table>

- **Domain**: The domain in which the MAC address was learned or statically configured.
- **Vlan/SrvcId/[ISId/vnID]**: The L2 GRE service ID number and the GRE tunnel VPN ID number associated with the L2 GRE service ID.
- **Mac Address**: MAC address that is currently learned or statically assigned.
- **Type**: MAC address management status (**dynamic, static, bmac**).
- **Operation**: The disposition of the MAC address (**bridging, filtering, servicing, quarantined**).
- **Interface**: The L2 GRE tunnel Service Access Point (SAP) or Service Distribution Point (SDP) associated with the MAC address.
**Release History**

Release 8.4.1.R02; command introduced.

**Related Commands**

- **show mac-learning**
  Displays Source Learning MAC Address Table information for the switch.

- **show mac-learning domain vlan**
  Displays MAC Address Table information for the VLAN source learning domain.

- **show mac-learning domain spb**
  Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.

- **show mac-learning domain vxlan**
  Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.

- **show mac-learning aging-time**
  Displays the current aging time value for the Source Learning MAC Address Table.

**MIB Objects**

- alaSlMacAddressGlobalTable
  - slMacDomain
  - slLocaleType
  - slOriginId
  - slServiceId
  - slSubId
  - slMacAddressGb1
  - slMacAddressGb1Management
  - slMacAddressGb1Disposition
  - slMacAddressGb1RowStatus
  - slMacAddressGb1GroupField
  - slL2GreVpnID
show mac-learning domain local

Displays MAC Address Table information for the local service source learning domain.

```
show mac-learning domain local [serviceid service_id] [sap chassis/slot/port:encap | dynamic | static | mac-address mac_address] [summary]
```

**Syntax Definitions**

- `service_id`: An existing service ID.
- `chassis/slot/port:encap`: The service access port and encapsulation (0, all, qtag, or outer_qtag.inner_qtag) for the local Service Access Point (SAP). For example, 1/1/2:10.
- `dynamic`: Displays dynamically learned MAC addresses.
- `static`: Displays static MAC addresses with a permanent status.
- `mac_address`: A MAC Address (for example, 00:00:39:59:f1:0c).
- `summary`: Displays a summary count of the MAC addresses known to the MAC address table for the specified domain.

**Defaults**

By default, all MAC address entries learned for the local domain are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a static MAC address is configured on a port link that is down or disabled, an asterisk appears to the right of the MAC address in the command display. The asterisk indicates that this is an invalid MAC address. When the port link comes up, however, the MAC address is then considered valid and the asterisk no longer appears next to the address in the display.
- If there is a duplicate static MAC address occurrence, an “&” symbol will appear to the right of the address in the command display.

**Examples**

```
-> show mac-learning domain local summary
Mac Address Table Summary:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Static</th>
<th>Static-Multicast</th>
<th>Bmac</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>
```
Source Learning Commands

show mac-learning domain local

Total MAC Address In Use = 7

-> show mac-learning domain local
Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL</td>
<td>1000 e8:e7:32:11:db:72</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:1/1/13:1000</td>
</tr>
<tr>
<td>LOCAL</td>
<td>1000 e8:e7:32:40:10:7e</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:32867:1000</td>
</tr>
<tr>
<td>LOCAL</td>
<td>1000 e8:e7:32:00:27:e1</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:32904:1000</td>
</tr>
<tr>
<td>LOCAL</td>
<td>1000 e8:e7:32:00:27:ee</td>
<td>dynamic</td>
<td>servicing</td>
<td>sdp:32904:1000</td>
</tr>
<tr>
<td>LOCAL</td>
<td>3899 e8:e7:32:42:e0:4d</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/99:99</td>
</tr>
<tr>
<td>LOCAL</td>
<td>3899 e8:e7:32:42:e0:5c</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/99:99</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 7

-> show mac-learning domain local serviceid 3899
Legend: Mac Address: * = address not valid,

<table>
<thead>
<tr>
<th>Domain Vlan/SrvcId/[ISId/vnID]</th>
<th>Mac Address</th>
<th>Type</th>
<th>Operation</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL</td>
<td>3899 e8:e7:32:42:e0:4d</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/99:99</td>
</tr>
<tr>
<td>LOCAL</td>
<td>3899 e8:e7:32:42:e0:5c</td>
<td>dynamic</td>
<td>servicing</td>
<td>sap:0/99:99</td>
</tr>
</tbody>
</table>

Total number of Valid MAC addresses above = 2

output definitions

<table>
<thead>
<tr>
<th>Domain</th>
<th>The domain in which the MAC address was learned or statically configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan/SrvcId/[ISId/vnID]</td>
<td>The service ID number associated with the MAC address.</td>
</tr>
<tr>
<td>Mac Address</td>
<td>MAC address that is currently learned or statically assigned.</td>
</tr>
<tr>
<td>Type</td>
<td>MAC address management status (dynamic, static, bmac).</td>
</tr>
<tr>
<td>Operation</td>
<td>The disposition of the MAC address (bridging, filtering, servicing, quarantined).</td>
</tr>
<tr>
<td>Interface</td>
<td>The service access point (SAP) associated with the MAC address.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Release 7.3.1; show command display modified to include domain and service information.
**Related Commands**

- **show mac-learning** Displays Source Learning MAC Address Table information for the switch.
- **show mac-learning domain vlan** Displays MAC Address Table information for the VLAN source learning domain.
- **show mac-learning domain spb** Displays MAC Address Table information for the Shortest Path Bridging (SPB) source learning domain.
- **show mac-learning domain vxlan** Displays MAC Address Table information for the Virtual eXtensible LAN (VXLAN) source learning domain.
- **show mac-learning domain l2gre** Displays MAC Address Table information for the L2 GRE tunnel source learning domain.
- **show mac-learning aging-time** Displays the current aging time value for the Source Learning MAC Address Table.

**MIB Objects**

- alaSlMacAddressGlobalTable
  - slMacDomain
  - slLocaleType
  - slOriginId
  - slServiceId
  - slSubId
  - slMacAddressGbl
  - slMacAddressGblManagement
  - slMacAddressGblDisposition
  - slMacAddressGblRowStatus
  - slMacAddressGblGroupField
  - slSvcISID
show mac-learning aging-time

Displays the current aging time value for the Source Learning MAC Address Table.

show mac-learning aging-time

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Note that the aging time is the same for all VLANs because it is not configurable on a per-VLAN basis. The aging time value on this platform is a global parameter that applies to all VLANs.

Examples

-> show mac-learning aging-time
Mac Address Aging Time (seconds) = 300

Release History

Release 7.1.1; command introduced.

Related Commands

show mac-learning Displays Source Learning MAC Address Table information.

MIB Objects

s1MacAddressAgingTable
s1MacAgingValue
**show mac-learning learning-state**

Displays the source learning status of a VLAN, port, or link aggregate.

```
show mac-learning learning-state [vlan vlan[1-vlan2] | port chassis/slot/port | linkagg agg_id]
```

**Syntax Definitions**

- **vlan**
  - The VLAN ID number.

- **-vlan2**
  - The last VLAN ID in a range of VLAN IDs.

- **chassis**
  - The chassis identifier.

- **slot/port**
  - The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

- **agg_id**
  - Specifies the link aggregate identifier.

**Defaults**

By default, the source learning status for all switch ports and link aggregates is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **port** or **linkagg** keywords along with the port ID and link aggregate ID to display the source learning status for a specific port or link aggregate ID.

- Use the **vlan** keyword along with the VLAN ID or a range of VLAN IDs to display the source learning status for the specified VLAN or range of VLANs.

- Output display for a range of port IDs is supported with this command. However, output display for a range of link aggregate IDs is not supported.

- When the source learning status is configured for a link aggregate ID, it affects all the ports that are members of the link aggregate. However, the source learning status cannot be configured on individual ports which are members of the link aggregate.

**Example**

```
-> show mac-learning learning-state

port source-learning
----------
1/1       disabled
```
1/2    enabled
1/3    disabled

-> show mac-learning learning-state port 1/2

port  source-learning
-----+----------------
1/2    enabled

-> show mac-learning learning-state linkagg 10

port  source-learning
-----+----------------
0/10   disabled

**output definitions**

<table>
<thead>
<tr>
<th>port</th>
<th>The slot/port number for a switch port or a link aggregate ID number. If the interface is a link aggregate ID, zero is displayed as the slot number (for example, 0/29).</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-learning</td>
<td>The source learning status of the port or link aggregate (<strong>enabled</strong> or <strong>disabled</strong>). Configured through the <strong>mac-learning</strong> command.</td>
</tr>
</tbody>
</table>

-> show mac-learning learning-state vlan 1-5

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Learning State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
</tr>
<tr>
<td>5</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Vlan</th>
<th>The VLAN ID numbers of the VLANs that are active.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learning State</td>
<td>The MAC learning state of the VLANs.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **mac-learning** Configures the status of source MAC address learning on a single port, a range of ports or on a link aggregate of ports.

**MIB Objects**

- slMacAddressTable
  - slMacLearningControlTable
  - slMacLearningControlEntry
  - slMacLearningControlStatus
show mac-learning mode

Displays the current source learning mode (centralized or distributed) for the switch.

show mac-learning mode

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
Not supported in this release.

Usage Guidelines
N/A

Examples
-> show mac-learning mode
MAC Learning Mode Configuration = CENTRALIZED
New Configured MAC Learning Mode After Reboot = DISTRIBUTED

-> show mac-learning mode
MAC Learning Mode Configuration = DISTRIBUTED

Release History
Release 7.1.1; command introduced.

Related Commands
mac-learning mode Enables or disables the distributed MAC source learning mode.

MIB Objects
slMacAddressTable
    slDistributedMacMode
mac-ping

Configure a MAC address ping for testing Layer 2 connectivity.

```
mac-ping dst-mac mac_address vlan vlan_id [priority vlan_priority] [drop-eligible {true | false}] [count count] [interval delay] [size size] [isid-check isid]
```

**Syntax Definitions**

- **mac**
  The destination MAC address to ping.

- **vlan-id**
  The VLAN on which the packets will be sent out. Valid range is 1-4094.

- **vlan-priority**
  Specifies both the internal priority of the Mac ping and the 802.1p value on the vlan tag header. Valid range is 0-7.

- **true | false**
  Specifies both the internal drop precedence of the MAC ping and the CFI bit on the vlan tag header. Default is false.

- **count**
  The number of packets to send in one ping iteration. Valid range is 1–5.

- **delay**
  The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100 ms to 1000 ms in multiples of 100 ms.

- **size**
  The size of the ICMP payload to be used for the ping iteration. Valid range is 32–1500 bytes.

- **isid**
  A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-priority</td>
<td>0</td>
</tr>
<tr>
<td>drop-eligible</td>
<td>false</td>
</tr>
<tr>
<td>count</td>
<td>5</td>
</tr>
<tr>
<td>delay</td>
<td>1000 ms</td>
</tr>
<tr>
<td>size</td>
<td>36 bytes</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The timeout for each ping request packet is one second. This value is not configurable.
- Destination MAC cannot be a broadcast, multicast, or NULL address.
- Enable the Network Time Protocol (NTP) using the NTP client command for a MAC address ping to work correctly across Virtual Chassis.

**Examples**

-> mac-ping dst-mac 00:11:11:11:11:11 vlan 10  
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 10 count 5 size 100  
-> mac-ping dst-mac 00:11:11:11:11:11 vlan 1001 isid-check 1002

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **show mac-learning** Displays Source Learning MAC Address Table information.

**MIB Objects**

N/A
5  VLAN Management Commands

VLAN management software handles VLAN configuration and the reporting of VLAN configuration changes to other switch tasks. A VLAN defines a broadcast domain that contains physical ports and can span across multiple switches. All switches contain a default VLAN 1. Physical switch ports are initially assigned to VLAN 1 until they are statically or dynamically assigned to other VLANs.

This chapter includes descriptions of VLAN management commands used to create, modify or remove VLANs. These commands allow you to enable or disable Spanning Tree Protocol (STP), add or remove virtual router interfaces, statically assign physical switch ports to a default VLAN, and display VLAN configuration information.

MIB information is as follows:

Filename:  ALCATEL-IND1-VLAN-MGR-MIB.mib  
Module:  alcatelIND1VLANManagerMIB

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>VLAN Management Commands</th>
<th>pvlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>vlan</td>
</tr>
<tr>
<td>vlan members untagged</td>
<td>vlan members</td>
</tr>
<tr>
<td>vlan members tagged</td>
<td>vlan</td>
</tr>
<tr>
<td>vlan mtu-ip</td>
<td>mtu-ip</td>
</tr>
<tr>
<td>show vlan</td>
<td>show vlan</td>
</tr>
<tr>
<td>show vlan members</td>
<td>show</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Private VLAN Commands</th>
<th>pvlan secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>pvlan</td>
<td>pvlan</td>
</tr>
<tr>
<td>pvlan secondary</td>
<td>secondary</td>
</tr>
<tr>
<td>pvlan members</td>
<td>members</td>
</tr>
<tr>
<td>show pvlan</td>
<td>show pvlan</td>
</tr>
<tr>
<td>show pvlan mapping</td>
<td>show pvlan</td>
</tr>
<tr>
<td>show pvlan members</td>
<td>show pvlan</td>
</tr>
</tbody>
</table>
**vlan**

Creates a new VLAN with the specified VLAN ID (VID) and an optional description.

```
vlan vlan_id [admin-state {enable | disable}] [name description]
no vlan vlan_id
```

---

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>A numeric value that uniquely identifies an individual VLAN. This value becomes the VLAN ID for the new VLAN.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enable VLAN administrative status.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disable VLAN administrative status.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>An alphanumeric string. Optional name description for the VLAN ID.</td>
</tr>
</tbody>
</table>

---

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td><code>enable</code></td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- Use the **no** form of this command to delete a VLAN from the configuration.
- All VLAN ports and routers are detached before the VLAN is removed. If the VLAN deleted is a default VLAN on the port, the port returns to default VLAN 1.
- If the VLAN deleted is not a default VLAN, then the ports are directly detached from the VLAN.
- A VLAN is not operationally active until at least one of the member ports of the VLAN is active and can forward traffic.
- Note that specifying multiple VLAN IDs and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range of VLAN ID entries (for example, `vlan 10-15`).
- When a VLAN is administratively disabled, static port assignments are retained but traffic is not forwarded from these ports.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with space in between.
### Examples

```
-> vlan 200 name "Corporate VLAN"
-> vlan 720 admin-state disable
-> no vlan 1020
```

### Release History

Release 7.1.1; command introduced.

### Related Commands

- `vlan members untagged` Statically assigns ports to a VLAN.
- `show vlan` Displays a list of existing VLANs.
- `show vlan members` Displays VLAN port assignments.

### MIB Objects

- `vlanTable`
  - `vlanNumber`
  - `vlanDescription`
  - `vlanAdmStatus`
  - `vlanOperStatus`
  - `vlanStatus`
vlans return to the VLAN configuration prompt.

The chassis identifier.

An existing VLAN ID number of the VLAN to assign as the default VLAN configured for the port.

The slot number for the module and the physical port number (for example, 3/1 specifies port 1 on slot 3) or a range of physical port numbers on that module (for example, 3/1-16).

The link aggregate ID number or range of IDs to be assigned to the specified VLAN.

VLAN 1 is the default VLAN for all ports.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove a port or link aggregate from its configured default VLAN and restore VLAN 1 as the default VLAN.
- The VLAN ID and link aggregate ID specified with this command must already exist in the switch configuration.
- This command configures the port or link aggregate to send and receive untagged packets for the specified VLAN ID, which becomes the default VLAN of the port.
- Every switch port or link aggregate has only one configured default VLAN. The 802.1Q tagged ports, however, can have additional VLAN assignments, which are often referred to as secondary VLANs.
- NNI interface can be configured with normal VLANs (other than VLAN 1). This allows NNI ports to carry untagged packets for the specified VLAN ID.
  - If an interface is already an untagged member of a standard VLAN other than VLAN 1, then on
making it an NNI interface, there will be no change in the default VLAN of the interface.

- If the default VLAN is removed from the NNI interface, then the default VLAN would automatically change to 4095 for the NNI port, either physical or logical.
- Untagged packets ingressing on the NNI interface (whose default VLAN is other than 4095) shall be forwarded on the default VLAN on the NNI interface.

**Examples**

- `vlan 20 members port 4/1-24 tagged`
- `vlan 20 members linkagg 2-4 untagged`
- `no vlan 1-4 members port 4/1-24`
- `no vlan 20 members linkagg 2-4`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **vlan**
  - Creates a VLAN.
- **vlan members tagged**
  - Configures a port to accept 802.1q-tagged packets for a specific VLAN.
- **show vlan**
  - Displays list of existing VLANs.
- **show vlan members**
  - Displays VLAN port assignments.

**MIB Objects**

- **vpaTable**
  - **vpaVlanNumber**
  - **vpaIfIndex**
  - **vpaType**
  - **vpaState**
  - **vpaStatus**
**VLAN Management Commands**

**VLAN members tagged**

Configures a port or link aggregate ID to send and receive 802.1q-tagged packets with the specified VLAN ID.

```
vlan vlan_id[-vlan_id] members {port chassis/slot/port[-port] | linkagg agg_id[-agg_id]} tagged
```

```
no vlan vlan_id[-vlan_id] members {port chassis/slot/port[-port] | linkagg agg_id[-agg_id]}
```

### Syntax Definitions

- **vlan_id**
  - The VLAN ID number for a pre-configured VLAN that will handle the 802.1Q-tagged traffic for this port. Use a hyphen to specify a range of VLAN IDs (for example, `vlan 10-15`). The valid range is 1–4094.

- **chassis**
  - The chassis identifier.

- **slot/port[-port]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-10).

- **agg_id[-agg_id]**
  - A link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

### Defaults

By default, all ports are untagged (they only carry untagged traffic for the default VLAN to which the port belongs).

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to delete 802.1Q tagging on a port or an aggregate of ports.

- The VLAN ID and link aggregate ID specified with this command must already exist in the switch configuration.

- A port or link aggregate cannot be tagged with its own default VLAN ID.

- NNI interface can be tagged with normal VLANs. This allows NNI ports to carry regular 802.1q tagged traffic as well as SVLAN tagged traffic.
  - 802.1q VLAN tagging to an NNI interface will not be allowed if the interface is set with TPID other than 0x8100.
  - Tagged packets ingressing on the NNI interface (default VLAN other than 4095), with TPID other than the one configured on the interface shall be forwarded on the default VLAN of the
NNI interface.

- The TPID (other than 0x8100) of a NNI interface cannot be modified if the interface is already a tagged member of a legacy VLAN.

**Examples**

- `vlan 100 members port 3/1 tagged`
- `vlan 100 members port 4/1-10 tagged`
- `vlan 100 members linkagg 10 tagged`
- `vlan 100 members linkagg 1-4 tagged`
- `no vlan 100 members port 3/1`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `vlan` Creates a VLAN.
- `vlan members untagged` Configures the default VLAN for the specified port or link aggregate.
- `show vlan members` Displays VLAN port assignments.

**MIB Objects**

- `qPortVlanTable`
- `qPortVlanSlot`
- `qPortVlanPort`
- `qPortVlanStatus`
- `qPortVlanTagValue`
- `qPortVlanDescription`
- `qAggregateVlanTagValue`
- `qAggregateVlanAggregateId`
- `qAggregateVlanStatus`
- `qAggregateVlanDescription`
**vlan mtu-ip**

Configures the maximum transmission unit (MTU) packet size allowed for all ports associated with a VLAN. This value is configured on a per VLAN basis, so all IP interfaces assigned to the VLAN apply the same MTU value to packets sent on VLAN ports.

`vlan vlan_id mtu-ip size`

**Syntax Definitions**

- **vlan_id**: An existing VLAN ID number of the VLAN to assign as the default VLAN configured for the port.
- **size**: Packet size value specified in bytes.

**Defaults**

By default, the MTU size is set to 1500 bytes (the standard Ethernet MTU size).

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The MTU size applies to traffic sent on all switch ports that are associated with the specified VLAN regardless of the port speed (for example, 10/100 Ethernet, Gigabit Ethernet). Therefore, assign only ports that are capable of handling the MTU size restriction to the VLAN. If the VLAN MTU size is greater than 1500, do not assign 10/100 Ethernet ports to the VLAN.

- By default, packets that exceed the MTU size are dropped. To enable MTU discovery and fragmentation, use the `icmp type` command to enable the “frag needed but DF bit set” control (for example, `icmp type 3 code 4 enable`).

- The maximum MTU size value for a VLAN is 9198.

**Examples**

- `-> vlan 200 mtu-ip 1280`
- `-> vlan 1503 mtu-ip 9198`

**Release History**

Release 7.1.1; command introduced.
Related Commands

- `vlan` Creates a VLAN.
- `vlan members tagged` Configures a port to accept 802.1q-tagged packets for a specific VLAN.
- `show vlan` Displays list of existing VLANs.

MIB objects

- `vlanTable`
  - `vlanMtu`
show vlan

Displays a list of VLANs configured on the switch.

`show vlan [vlan_id]`

**Syntax Definitions**

`vlan_id`  
VLAN ID number.

**Defaults**

By default, a list of all VLANs is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify a VLAN ID with this command to display information about a specific VLAN.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, `show vlan 10-15`). Note that only one VLAN entry - a single VLAN ID or a range of VLAN IDs is allowed with this command. Multiple entries are not accepted.

**Examples**

```
-> show vlan

vlan  type   admin  oper  ip   mtu  name
-----+-------+-----+-----+-----+-----+---------------------
 1     std   Ena  Dis  Dis   1500 Finance IP
10    unpd  Ena  Dis  Dis   1500 UNP-DYN-VLAN
11    std   Ena  Dis  Dis   1500 VLAN 11
400   spb   Ena  Dis  Dis   1524 VLAN 500
500   fcoe  Ena  Dis  Dis   1500 VLAN 500
600   pvlan-p Ena  Dis  Dis   1500 PVLAN 600
601   pvlan-c Ena  Dis  Dis   1500 PVLAN 601
602   pvlan-i Ena  Dis  Dis   1500 PVLAN 602
```
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VLAN Management Commands</strong></td>
<td>show vlan</td>
</tr>
<tr>
<td><strong>output definitions</strong></td>
<td>The user-defined text description for the VLAN. By default, the VLAN ID is displayed if the VLAN description is not specified.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>The type of VLAN (such as Static VLAN, MTP VLAN, VCM IPC, VIP VLAN, UNP Dynamic VLAN, Backbone VLAN, Fibre Channel over Ethernet VLAN, PVLAN Primary vlan)</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>VLAN administrative status: enabled VLAN functions are enabled; disabled specifies that VLAN functions are disabled. Use the <code>vlan</code> command to change the VLAN administrative status.</td>
</tr>
<tr>
<td><strong>Administrative State</strong></td>
<td>VLAN operational status: enabled or disabled. The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow.</td>
</tr>
<tr>
<td><strong>Operational State</strong></td>
<td>The numerical VLAN ID. Use the <code>vlan</code> command to create or remove VLANs.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>The type of VLAN (mtp, vcm, std, unpd, spb, fcoe, pvlan-p, pvlan-e, pvlan-i). This field also displays the VLANs created through other applications, such as Shortest Path Bridging (SPB), VLAN Stacking, Fibre Channel over Ethernet (FCoE), and Private VLANs (PVLAN).</td>
</tr>
<tr>
<td><strong>admin</strong></td>
<td>VLAN administrative status: Ena specifies that VLAN functions are enabled; Dis specifies that VLAN functions are disabled. Use the <code>vlan</code> command to change the VLAN administrative status.</td>
</tr>
<tr>
<td><strong>oper</strong></td>
<td>VLAN operational status: Ena (enabled) or Dis (disabled). The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.</td>
</tr>
<tr>
<td><strong>ip</strong></td>
<td>IP router interface status: Ena (IP interface exists for the VLAN) or Dis (no IP router interface exists for the VLAN). Use the <code>ip interface</code> command to define an IP router interface for a VLAN.</td>
</tr>
<tr>
<td><strong>mtu</strong></td>
<td>Maximum Transmission Unit: Size of largest data packet that the VLAN port can transmit. Configured through the <code>vlan mtu-ip</code> command.</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>The user-defined text description for the VLAN. By default, the VLAN ID is displayed if the VLAN description is not specified. Configured through the <code>vlan</code> command.</td>
</tr>
</tbody>
</table>

```bash
-> show vlan 600
Name           : PVLAN 600,
Type           : PVLAN Primary vlan,
Administrative State : enabled,
Operational State    : disabled,
IP Routing         : disabled,
IP MTU            : 1500
MAC Tunneling     : disabled,
```
**output definitions**

| IP Routing | IP routing status: **enabled** (IP interface exists for the VLAN) or **disabled** (no IP interface exists for the VLAN). Use the `ip interface` command to define an IP router interface for a VLAN. |
| IP MTU | Maximum Transmission Unit: Size of largest data packet that the VLAN port can transmit. |
| MAC Tunneling | MAC tunneling status for the VLAN Stacking SVLAN: **enabled** or **disabled**. Use the `ethernet-service svlan mac-tunneling` to change the MAC tunneling status for the SVLAN. |

**Release History**

Release 7.1.1; command introduced.
Release 8.6R1; “MAC Tunneling” field added.
Release 8.7R1; “IP Router Port” field changed to “IP Routing”

**Related Commands**

- `show vlan members` Displays VLAN port assignments.

**MIB Objects**

- `vlanTable`
  - `vlanNumber`
  - `vlanDescription`
  - `vlanAdmStatus`
  - `vlanOperStatus`
  - `vlanRouterStatus`
  - `vlanType`
  - `vlanMtu`
  - `vlanMacTunneling`
**show vlan members**

Displays VLAN-port associations (VPAs) for all VLANs, a specific VLAN, or for a specific port.

```plaintext
show vlan [vlan_id[-vlan_id]] members [port chassis/slot/port[-port]] linkagg agg_id[-agg_id]]
```

### Syntax Definitions

- **vlan_id**: VLAN ID number. Use a hyphen to specify a range of VLAN IDs (for example, `vlan 10-15`).
- **chassis**: The chassis identifier.
- **slot/port[-port]**: The slot and port number (3/1) of a specific interface to display. Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id]**: Enter a link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs.

### Defaults

If no parameters are specified with this command, a list of all VLANs and their assigned ports is displayed by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If the `vlan_id` is specified without a `slot/port` or `agg_id`, then all port assignments for that VLAN are displayed.
- If the `slot/port` or `agg_id` is specified without a `vlan_id`, then all VLAN assignments for that port are displayed.
- If both the `vlan_id` and `slot/port` or `agg_id` are specified, then information only for that VLAN and slot/port or link aggregate ID is displayed.
- Note that specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (for example, `show vlan 10-15 port`). Note that only one VLAN entry - a single VLAN ID or a range of VLAN IDs is allowed with this command. Multiple entries are not accepted.
- The following types of VPAs may appear in the “type” field based on the switch configuration:

<table>
<thead>
<tr>
<th>VPA Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>untagged</td>
<td>Statically configured untagged VLAN assignment for the port.</td>
</tr>
</tbody>
</table>
### VLAN Management Commands

**show vlan members**

#### Examples

```plaintext
-> show vlan members

<table>
<thead>
<tr>
<th>vlan</th>
<th>port</th>
<th>type</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/1</td>
<td>untagged</td>
<td>inactive</td>
</tr>
<tr>
<td>2</td>
<td>1/2</td>
<td>untagged</td>
<td>blocking</td>
</tr>
<tr>
<td>3</td>
<td>1/2</td>
<td>tagged</td>
<td>forwarding</td>
</tr>
<tr>
<td></td>
<td>11/4</td>
<td>tagged</td>
<td>forwarding</td>
</tr>
<tr>
<td>2</td>
<td>2/5</td>
<td>dynamic</td>
<td>forwarding</td>
</tr>
</tbody>
</table>
```

```plaintext
-> show vlan 10 members

<table>
<thead>
<tr>
<th>port</th>
<th>type</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>untagged</td>
<td>forwarding</td>
</tr>
<tr>
<td>1/2</td>
<td>tagged</td>
<td>forwarding</td>
</tr>
</tbody>
</table>
```

```plaintext
-> show vlan members port 3/2

<table>
<thead>
<tr>
<th>vlan</th>
<th>type</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>untagged</td>
<td>forwarding</td>
</tr>
<tr>
<td>2</td>
<td>tagged</td>
<td>forwarding</td>
</tr>
<tr>
<td>5</td>
<td>dynamic</td>
<td>blocking</td>
</tr>
<tr>
<td>3</td>
<td>tagged</td>
<td>blocking</td>
</tr>
</tbody>
</table>
```

```plaintext
-> show vlan 1-11 members port 1/3

type : untagged,
status : inactive,
vlan admin : enabled,
vlan oper : disabled,
```

#### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Numerical VLAN ID. Identifies the VLAN assignment of the port.</td>
</tr>
<tr>
<td>port</td>
<td>The slot number for the module and the physical port number on that module (for example 3/1 specifies port 1 on slot 3).</td>
</tr>
</tbody>
</table>
**VLAN Management Commands**

**show vlan members**

---

**Output Definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>The type of VPA: <strong>untagged</strong> (configured untagged VLAN assignment for the port), <strong>tagged</strong> (802.1Q-tagged secondary VLAN assignment for the port), <strong>mirror</strong> (port is mirroring the VLAN assignment of another port), <strong>dynamic</strong> (dynamically configured VLAN assignment for the port).</td>
</tr>
<tr>
<td><strong>status</strong></td>
<td>The VPA status: <strong>inactive</strong> (port is not active), <strong>forwarding</strong> (traffic is forwarding on this VPA), <strong>blocking</strong> (traffic is not forwarding on this VPA).</td>
</tr>
<tr>
<td><strong>vlan admin</strong></td>
<td>VLAN administrative status: <strong>enabled</strong> enables VLAN functions to operate; <strong>disabled</strong> disables VLAN functions without deleting the VLAN. Use the <strong>vlan</strong> command to change the VLAN administrative status.</td>
</tr>
<tr>
<td><strong>vlan oper</strong></td>
<td>VLAN operational status: <strong>enabled</strong> or <strong>disabled</strong>. The operational status remains disabled until an active port is assigned to the VLAN. When the operational status is enabled, then VLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow. A VLAN must have an enabled administrative status before it can become operationally enabled.</td>
</tr>
</tbody>
</table>

---

**Release History**

Release 7.1.1; command introduced.
Release 8.9R1; output fields ‘default’ changed to ‘untagged’, ‘qtagged’ changed to ‘tagged’.

**Related Commands**

- **show vlan** Displays list of VLANs configured on the switch.
- **show ip interface** Displays IP router information.

**MIB Objects**

- **vlanMgrVpa**
- **vpaTable**
  - **vpaVlanNumber**
  - **vpaIfIndex**
  - **vpaType**
  - **vpaState**
  - **vpaStatus**
- **vlanMgrVlan**
- **vlanTable**
  - **vlanAdmStatus**
  - **vlanOperStatus**
**pvlan**

Creates a new Private VLAN (PVLAN) with the specified VLAN ID and an optional description. The specified VLAN ID will serve as the Primary VLAN for the PVLAN configuration.

```
pvlan vlan_id[-vlan_id] [admin-state {enable | disable}] [name description] mtu-ip size
```

```
no pvlan vlan_id[-vlan_id]
```

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>A numeric value that uniquely identifies the PVLAN. The valid range 2–4094.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enable the VLAN administrative status.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disable VLAN administrative status.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>An alphanumeric string. Optional name description for the PVLAN.</td>
</tr>
<tr>
<td><code>size</code></td>
<td>The Maximum Transfer Unit (MTU) size for the PVLAN.</td>
</tr>
</tbody>
</table>

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Specify a VLAN ID that does not already exist in the switch configuration.
- Use a hyphen to indicate a contiguous range of VLAN ID entries.
- Enclose the description in double quotes if it contains more than one word with a space in between each word.
- The `capability shared-vlan-learning` command must be enabled on the OS6860N and OS6900-X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 models when configuring PVLAN.

---

**Examples**

- `-> pvlan 200 name "Corporate PVLAN"`
- `-> pvlan 200 admin-state disable`
- `-> pvlan 300-302 admin-state enable`
Release History

Release 8.3.1; command introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pvlan secondary</td>
<td>Creates a new Secondary VLAN and associates it with the Primary VLAN in a PVLAN configuration.</td>
</tr>
<tr>
<td>pvlan members</td>
<td>Assigns ports or link aggregates to a Primary or Secondary VLAN in a PVLAN configuration.</td>
</tr>
<tr>
<td>show pvlan</td>
<td>Displays a list of PVLANs configured on the switch.</td>
</tr>
<tr>
<td>show pvlan mapping</td>
<td>Displays the Primary VLAN and Secondary VLAN mapping.</td>
</tr>
<tr>
<td>show pvlan members</td>
<td>Displays VPAs for all or specific VLANs in a PVLAN configuration.</td>
</tr>
<tr>
<td>capability shared-vlan-learning</td>
<td>Enables or disables shared VLAN learning.</td>
</tr>
</tbody>
</table>

MIB Objects

alaPrivateVlanTable
   - alaPrivateVlanID
   - alaPrivateVlanAdminState
   - alaPrivateVlanName
   - alaPrivateVlanType
   - alaPrivateVlanMtuIp
**pvlan secondary**

Creates a new Secondary VLAN and associates it with the Primary VLAN in a Private VLAN (PVLAN) configuration.

```
pvlan vlan_id secondary vlan_id[-vlan_id] type {isolated | community}
no pvlan vlan_id secondary vlan_id[-vlan_id]
```

**Syntax Definitions**

- **pvlan vlan_id**  
  A numeric value that uniquely identifies the Primary VLAN. The valid range is 2–4094.

- **secondary vlan_id**  
  A numeric value that uniquely identifies the Secondary VLAN to assign to the specified Primary VLAN. The valid range is 2–4094.

- **isolated**  
  Configures the secondary VLAN as an Isolated VLAN.

- **community**  
  Configures the secondary VLAN as a Community VLAN.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
|                | 6360           | 6465           | 6560           | 6570M          | 6860           | 6860N          | 6865           | 6900 V72/C32   |
|----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+----------------+
|                | No             | No             | No             | No             | Yes            | Yes            | Yes            | No             |
| No             | Yes            | Yes            | No             | Yes            | No             | Yes            | No             | No             |
```

**Usage Guidelines**

- Use the **no** form of the command to remove the Secondary VLAN assignment.
- The Primary VLAN ID must already exist.
- The Secondary VLAN ID must not already exist.
- Use a hyphen to indicate a contiguous range of VLAN ID entries.
- There can only be one Isolated Secondary VLAN associated with a Primary VLAN.

**Examples**

```bash
-> pvlan 200 secondary 250 type isolated
-> pvlan 200 secondary 251 type community
-> no pvlan 200 secondary 251
```
**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- **pvlan**
  Creates a new Primary VLAN with the specified VLAN ID and an optional description.

- **pvlan members**
  Assigns ports or link aggregates to a Primary or Secondary VLAN in a PVLAN configuration.

- **show pvlan**
  Displays a list of PVLANs configured on the switch.

- **show pvlan mapping**
  Displays the Primary VLAN and Secondary VLAN mapping.

- **show pvlan members**
  Displays VPAs for all or specific VLANs in a PVLAN configuration.

**MIB Objects**

alaPrivateVlanMappingTable

- alaPrivateVlanMappingPrimaryVlanID
- alaPrivateVlanMappingSecondaryVlanID
- alaPrivateVlanMappingSecondaryVlanType
pvlan members

Configures a tagged or untagged VLAN-port association (VPA) between ports or link aggregates and the specified VLAN ID in a Private VLAN (PVLAN) configuration.

```
 pvlan vlan_id members {port chassis/slot/port[-port] | linkagg agg_id[-agg_id]} {tagged | untagged} | isl
```

```
 no pvlan vlan_id members {port chassis/slot/port[-port] | linkagg agg_id[-agg_id]}
```

### Syntax Definitions

- **vlan_id**
  - A numeric value that uniquely identifies a Primary VLAN or Secondary VLAN in a PVLAN configuration. The valid range is 2–4094.
- **chassis**
  - The chassis identifier.
- **slot/port[-port]**
  - The slot and port number.
- **agg_id[-agg_id]**
  - The link aggregate ID number or range of IDs. The ID must be in the range 1 to 128.
- **tagged**
  - Configures the port or link aggregate ID to send and receive 802.1q-tagged packets with the specified PVLAN ID.
- **untagged**
  - Configures the port or link aggregate ID to send and receive non-802.1q-tagged packets.
- **isl**
  - Configures the port as an inter-switch link (ISL) port capable of carrying PVLAN traffic for all the VLANs that are members of a PVLAN between PVLAN-aware switches.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/</th>
<th>6900X48C8/C32E/T24C2/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to remove a port or link aggregate from the specified VLAN ID.
- The VLAN ID must already exist in the switch configuration.
- An ISL port can only be assigned to a Primary VLAN.
When a port is assigned to a PVLAN configuration, the port type is determined by the type of VLAN to which the port is assigned. For example:

- Ports assigned to a Primary VLAN are designated as promiscuous ports.
- Ports assigned to a Secondary VLAN configured as a Community VLAN are designated as community ports.
- Ports assigned to a Secondary VLAN configured as an Isolated VLAN are designated as isolated ports.

A port or link aggregate can only belong to one Primary VLAN or one Secondary VLAN at any given time. The exception to this is on the OmniSwitch 9900, where multiple VPAs for one port are allowed with the following conditions:

- Each VLAN tagged on the port must be of the same PVLAN type. For example, port 1/1/2 must belong to either all Primary VLANs, all Isolated Secondary VLANs, or all Community Secondary VLANs.
- Each VLAN tagged on the port must belong to a different PVLAN domain. For example, port 1/1/2 can be tagged with Primary VLAN 200 and Primary VLAN 300 because both VLANs are in separate PVLAN domains.

Only one untagged VPA is allowed per port.

On ports with only tagged VPAs, all untagged traffic is dropped.

Examples

- `pvlan 200 members port 1/1/1-5 tagged`
- `pvlan 200 members linkagg 2-4 untagged`
- `pvlan 200 members port 1/1/20 isl`
- `no pvlan 200 members port 1/1/1`
- `no pvlan 200 members linkagg 2`

Release History

Release 8.3.1; command introduced.

Related Commands

`pvlan` Creates a new Primary VLAN with the specified VLAN ID and an optional description.

`pvlan secondary` Creates a new Secondary VLAN that is assigned to a Primary VLAN.

`show pvlan` Displays a list of PVLANs configured on the switch.

`show pvlan mapping` Displays the Primary VLAN and Secondary VLAN mapping.

`show pvlan members` Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>alaPrivateVlanPortAssociationTable</code></td>
<td>Contains information about the association of a port with a PVLAN.</td>
</tr>
<tr>
<td><code>alaPrivateVlanPortAssociationVlanID</code></td>
<td>Specifies the VLAN ID associated with a port.</td>
</tr>
<tr>
<td><code>alaPrivateVlanPortAssociationPortIfIndex</code></td>
<td>Identifies the interface index of a port.</td>
</tr>
<tr>
<td><code>alaPrivateVlanPortAssociationVlanOption</code></td>
<td>Specifies VLAN options for a port.</td>
</tr>
<tr>
<td><code>alaPrivateVlanPortAssociationPortType</code></td>
<td>Specifies the port type.</td>
</tr>
</tbody>
</table>
show pvlan

Displays a list of Private VLANs (PVLANs) configured on the switch.

`show pvlan [vlan_id-vlan_id]`

**Syntax Definitions**

`vlan_id` PVLAN ID number.

**Defaults**

By default, a list of all PVLANs is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify a VLAN ID with this command to display information about a specific VLAN in a PVLAN configuration.

**Examples**

```
-> show pvlan
pvlan   type      admin   oper    mtu          name
------+----------+-------+------+------+------------------
200   Primary    Ena     Dis    1500   PVLAN 200
250   Isolated   Ena     Dis    1500   PVLAN 250
251   Community  Ena     Dis    1500   PVLAN 251
```

**output definitions**

`pvlan` The PVLAN ID.

`type` The type of PVLAN (Primary, Isolated, Community)

`admin` PVLAN administrative status: **Ena** specifies that PVLAN functions are enabled; **Dis** specifies that PVLAN functions are disabled.

`oper` PVLAN operational status: **Ena** (enabled) or **Dis** (disabled). The operational status remains disabled until an active port is assigned to the PVLAN. When the operational status is enabled, then PVLAN properties (for example router interfaces, Spanning Tree) are applied to ports and traffic flow. A PVLAN must have an enabled administrative status before it can become operationally enabled.
show pvlan

-> show pvlan 200
Name : PVLAN 200,
Type : PVLAN Primary vlan,
Administrative State : enabled,
Operational State : disabled,
IP MTU : 1500

Release History
Release 8.3.1; command introduced.

Related Commands
pvlan Creates a new Primary VLAN with the specified VLAN ID and an optional description.
pvlan secondary Creates a new Secondary VLAN that is assigned to a Primary VLAN.
show pvlan mapping Displays the Primary VLAN and Secondary PVLAN mapping.
show pvlan members Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects
alaPrivateVlanPrimaryVlanID
alaPrivateVlanType
alaPrivateVlanAdminState
alaPrivateVlanOperState
alaPrivateVlan
alaPrivateVlanName

output definitions (continued)

mtu The Maximum Transmission Unit size. Specifies the size of the largest data packet that the PVLAN port can transmit.
name The user-defined text description for the PVLAN. By default, the PVLAN ID is displayed if the PVLAN description is not specified.

output definitions

Name The user-defined text description for the PVLAN. By default, the PVLAN ID is displayed if the PVLAN description is not specified.
Type The type of PVLAN (Primary, Isolated, Community)
Administrative State PVLAN administrative status: enabled or disabled.
Operational State PVLAN operational status: enabled or disabled. The operational status remains disabled until an active port is assigned to the PVLAN.
IP MTU The Maximum Transmission Unit size. Specifies the size of the largest data packet that the PVLAN port can transmit.

mtu
The Maximum Transmission Unit size. Specifies the size of the largest data packet that the PVLAN port can transmit.

name
The user-defined text description for the PVLAN. By default, the PVLAN ID is displayed if the PVLAN description is not specified.

**show pvlan mapping**

Displays the Primary VLAN and Secondary PVLAN mapping in a Private VLAN (PVLAN) configuration.

**Syntax**

```
show pvlan [vlan_id] mapping
```

**Syntax Definitions**

- **vlan_id**: PVLAN ID number.

**Defaults**

If no parameters are specified with this command, the mapping for all PVLANs is displayed by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify a VLAN ID with this command to display information about a specific VLAN in a PVLAN configuration.

**Examples**

```
-> show pvlan mapping
Primary  Secondary
VLAN    VLAN    Type
----------+----------+----------
200      250    Isolated
200      251    Community
```

**output definitions**

- **Primary VLAN**: The VLAN ID of a Primary VLAN.
- **Secondary VLAN**: The VLAN ID of a Secondary VLAN that is mapped to the Primary VLAN ID.
- **Type**: The type of Secondary VLAN (*Primary, Isolated, Community*).

**Release History**

Release 8.3.1; command introduced.
Related Commands

**pvlan**  
Creates a new Primary VLAN with the specified VLAN ID and an optional description.

**pvlan secondary**  
Creates a new Secondary VLAN that is assigned to a Primary VLAN.

**show pvlan**  
Displays a list of PVLANs configured on the switch.

**show pvlan members**  
Displays VPAs for all or specific VLANs in a PVLAN configuration.

MIB Objects

- `alaPrivateVlanMappingPrimaryVlanID`
- `alaPrivateVlanMappingSecondaryVlanID`
- `alaPrivateVlanMappingSecondaryVlanType`
show pvlan members

Displays the VLAN-port associations (VPAs) for all or specific VLANs in a Private VLAN (PVLAN) configuration.

`show pvlan [vlan_id[-vlan_id]] members`

**Syntax Definitions**

`vlan_id`  VLAN ID or range of IDs.

**Defaults**

If no parameters are specified with this command, a list of all PVLANs and their assigned ports is displayed by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify a VLAN ID or the range of VLAN IDs with this command to display information about a specific VLAN or for the range of VLAN IDs.

**Examples**

```
-> show pvlan members
pvlan  port type     status      port-type
-------+----------------+------------+------------+------------+------------+------------+------------+------------+------------+------------+------------+
     200 | 1/10            untagged     inactive     promiscuous
     200 | 1/11            tagged       inactive     isl
     250 | 1/15            tagged       inactive     isolated
     251 | 1/16            untagged     inactive     community
     251 | 0/10            tagged       inactive     community
```

```
-> show pvlan 200 members
port type     status      port-type
--------+----------------+------------+------------+------------+------------+------------+------------+------------+------------+------------+------------+
1/10    untagged     inactive     promiscuous
1/11    tagged       inactive     isl
0/10    tagged       inactive     promiscuous
```

**output definitions**

`pvlan`  The PVLAN ID.

`port`  The port number.
**output definitions**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>The type of VPA:</td>
</tr>
<tr>
<td>untagged</td>
<td>(configured default VLAN assignment for the port)</td>
</tr>
<tr>
<td>tagged</td>
<td>(802.1Q-tagged secondary VLAN assignment for the port)</td>
</tr>
<tr>
<td><strong>status</strong></td>
<td>The VPA status:</td>
</tr>
<tr>
<td>inactive</td>
<td>(port is not active)</td>
</tr>
<tr>
<td>forwarding</td>
<td>(traffic is forwarding on this VPA)</td>
</tr>
<tr>
<td>blocking</td>
<td>(traffic is not forwarding on this VPA)</td>
</tr>
<tr>
<td><strong>port-type</strong></td>
<td>The PVLAN port type:</td>
</tr>
<tr>
<td>Promiscuous</td>
<td>— A port which is a member of a Primary VLAN.</td>
</tr>
<tr>
<td>ISL</td>
<td>— A port carrying VLAN traffic for all the VLANs that are members</td>
</tr>
<tr>
<td></td>
<td>of a PVLAN between “PVLAN-aware” switches. (Isolated, Community, and</td>
</tr>
<tr>
<td></td>
<td>Promiscuous).</td>
</tr>
<tr>
<td>Community</td>
<td>— A port which is a member of a Community VLAN.</td>
</tr>
<tr>
<td>Isolated</td>
<td>— A port which is a member of an Isolated VLAN.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.3.1; command introduced.
Release 8.9R1; output fields ‘default’ changed to ‘untagged’, ‘qtagged’ changed to ‘tagged’.

**Related Commands**

- **pvlan**
  - Creates a new Primary VLAN with the specified VLAN ID and an optional description.
- **pvlan secondary**
  - Creates a new Secondary VLAN that is assigned to a Primary VLAN.
- **pvlan members**
  - Assigns ports or link aggregates to a Primary or Secondary VLAN in a PVLAN configuration.
- **show pvlan**
  - Displays a list of PVLANs configured on the switch.
- **show pvlan mapping**
  - Displays the Primary VLAN and Secondary VLAN mapping.

**MIB Objects**

- `alaPrivateVlanPortAssociationVlanID`
- `alaPrivateVlanPortAssociationPortIfIndex`
- `alaPrivateVlanPortAssociationVlanOption`
- `alaPrivateVlanPortAssociationPortStatus`
- `alaPrivateVlanPortAssociationPortType`
6 High Availability VLAN

Commands

High availability (HA) VLANs send traffic intended for a single destination MAC address to multiple switch ports. The OmniSwitch HA VLAN feature provides an elegant and flexible way to connect server cluster nodes directly to the ingress network. This involves multicasting the service requests on the configured ports. The multicast criteria is configurable based on destination MAC and destination IP address. Egress ports can be statically configured on a server cluster or they can be registered by IGMP reports. The HA VLAN server cluster feature multicasts the incoming packets based on the server cluster configuration on the ports associated with the server cluster.

An HAVLAN is configured by specifying the match criteria, a VLAN and a port list. Match criteria is used to identify the incoming traffic that has to be processed by the HA VLAN server-clusters. The specified VLAN is an ingress and egress VLAN in the case of a L2 server-cluster. In the case of a L3 server-cluster, the VLAN is not configured explicitly, but the IP address specified in the match criteria determines the VLAN. The port list specifies the egress switch ports within the VLAN. The cluster is connected to these switch ports.

There are typically two modes of implementation of server clusters in HA VLAN.

**Layer 2** - The server cluster is attached to a L2 switch on which the frames destined to the cluster MAC address are to be flooded on all interfaces.

**Layer 3** - The server cluster is attached to a L3 switch on which the frames destined to the server cluster IP address are to be routed to the server cluster IP and then flooded on all interfaces.

For more information, see the application examples in Chapter 28, “Configuring High Availability VLANs” in the OmniSwitch AOS Release 8 Network Configuration Guide.

MIB information is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-VLAN-MGR-MIB.mib</td>
<td>alcatelIND1VLANManagerMIB</td>
</tr>
<tr>
<td>ALCATEL-IND1-MAC-ADDRESS-MIB.mib</td>
<td>alcatelIND1MacAddressMIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:

```
server-cluster
server-cluster vlan
server-cluster mac-address
server-cluster ip
server-cluster igmp mode
server-cluster ip-multicast
server-cluster port
show server-cluster
```
server-cluster

Configures a cluster with an ID, name, mode and the administrative state.

```
server-cluster cluster_id [name cluster_name] [mode {L2 | L3}] [admin-state {enable | disable}]
no server-cluster cluster_id
```

**Syntax Definitions**

- `cluster_id` : A numerical identifier of the cluster. The valid range is 1–16.
- `cluster_name` : Specifies a name (up to 32 characters) to represent the cluster.
- `L2` : Specifies L2 for the cluster mode.
- `L3` : Specifies L3 for the cluster mode.
- `enable` : Enables the administrative state of the cluster.
- `disable` : Disables the administrative state of the cluster.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode</td>
<td>L2</td>
</tr>
<tr>
<td>admin-state</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>9000</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use **no** form of this command to remove the cluster ID from the switch configuration.
- Once the cluster mode is set, the mode cannot be changed.
- Use the **admin-state disable** parameter option to disable an existing cluster before attempting to modify any of the cluster parameters.

**Examples**

```
-> server-cluster 1
-> server-cluster 1 mode 12
-> server-cluster 1 name l2_cluster mode 12
-> server-cluster 2 name l3_cluster mode 13
-> no server-cluster 1
```
Release History

Release 7.2.1; command was introduced.

Related Commands

- vlan
  Creates and deletes VLANs.
- server-cluster mac-address
  Configures a MAC address, VLAN of the specified cluster.
- server-cluster port
  Configures the specified IP, ARP entry to a given cluster and/or a multicast IP.
- show server-cluster
  Displays the clusters configured in the system.

MIB Objects

alaHAVlanClusterTable
- alaHAVlanClusterId
- alaHAVlanClusterName
- alaHAVlanClusterAdminStatus
- alaHAVlanClusterMode
- alaHAVlanClusterRowStatus
server-cluster vlan

Configures a VLAN assignment for the specified cluster. This command is used to assign VLANs to an L2 cluster.

server-cluster cluster_id vlan vlan_id

Syntax Definitions

cluster_id

The numerical identifier of an existing server cluster.

vlan_id

The VLAN identifier to assign to the cluster. The valid range is 1–4094.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- If the specified VLAN ID does not exist in the switch configuration, the cluster will remain operationally disabled.
- Modifying the existing VLAN assignment for a cluster is only allowed when the cluster is administratively disabled.

Examples

- server-cluster 1 vlan 10
- server-cluster 5 vlan 10
- server-cluster 6 mac-address 00:11:22:33:44:55

Release History

Release 7.2.1; command was introduced.
Related Commands

server-cluster ip  Configures the specified IP, ARP entry to a given cluster.
server-cluster port  Configures the specified IP, ARP entry to a given cluster and/or a multicast IP.
show server-cluster  Displays the clusters configured in the system.
show mac-learning  Displays Source Learning MAC Address Table information.

MIB Objects

alaHAVlanClusterTable
   alaHAVlanClusterId
   alaHAVlanClusterVlan
   alaHAVlanClusterMacAddress
   alaHAVlanClusterRowStatus
server-cluster mac-address

Configures a MAC address assignment for the specified cluster. This command is used to assign a MAC address to an L2 cluster.

server-cluster cluster_id mac-address mac_address

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster_id</td>
<td>The numerical identifier of an existing server cluster.</td>
</tr>
<tr>
<td>mac_address</td>
<td>The MAC address of the cluster.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- Modifying the existing MAC address assignment for a cluster is only allowed when the cluster is administratively disabled.
- The MAC address that is assigned to a cluster can be a unicast, L2 multicast, or IP multicast address. However reserved multicast MAC addresses cannot be assigned to the cluster.
- The multicast addresses within the following reserved ranges are not supported:
  - 01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF
  - 01:80:C2:XX:XX:XX
  - 33:33:XX:XX:XX:XX

Examples

- server-cluster 1 vlan 10 mac-address 00:11:22:33:44
- server-cluster 5 vlan 10
- server-cluster 5 mac-address 01:
- server-cluster 6 mac-address 00:11:22:33:44:55

Release History

Release 7.2.1; command was introduced.
Related Commands

server-cluster ip       Configures the specified IP, ARP entry to a given cluster.
server-cluster port    Configures the port or linkagg to be assigned to a specific cluster.
show server-cluster    Displays the clusters configured in the system.
show mac-learning      Displays Source Learning MAC Address Table information.

MIB Objects

alaHAVlanClusterTable  
alaHAVlanClusterId     
alaHAVlanClusterVlan   
alaHAVlanClusterMacAddress 
alaHAVlanClusterRowStatus
**server-cluster ip**

Configures an IP address and ARP entry for the specified cluster. This command is used to assign an IP address to an L3 cluster.

```
server-cluster cluster_id ip ip_address [mac-address {static mac_address | dynamic}]
```

### Syntax Definitions

- **cluster_id**
  - The numerical identifier of an existing server cluster.

- **ip_address**
  - The unicast IP address to assign to the cluster.

- **mac_address**
  - The MAC address for the static ARP entry.

- **dynamic**
  - Dynamically resolve the ARP entry for the cluster.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td>X48C6/T48C6</td>
<td>X48C4E/V48C8</td>
<td>C32E/T24C2</td>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Release 7.2.1; command was introduced.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The cluster ID specified with this command must already exist in the switch configuration.
- A cluster can be assigned an IP address and ARP entry MAC address. Each cluster should have a unique IP address.
- Reserved MAC address cannot be configured as an ARP.
- Modifying the existing IP address parameters for a cluster is only allowed when the cluster is administratively disabled.

### Examples

- `-> server-cluster 1 ip 10.135.33.203 mac-address static 00 :11 :22 :33 :44`
- `-> server-cluster 3 ip 10.135.33.205 mac-address dynamic`
- `-> server-cluster 5 ip 10.135.33.207`
- `-> server-cluster 6 mac-address dynamic`
- `-> server-cluster 7 mac-address static 00 :11 :22 :33 :44`

### Release History

Release 7.2.1; command was introduced.
**Related Commands**

- `server-cluster mac-address`  
  Configures a MAC address of the specified cluster.

- `server-cluster port`  
  Configures the port or linkagg to be assigned to a specific cluster.

- `show server-cluster`  
  Displays the clusters configured in the system.

**MIB Objects**

- `alaHAVlanClusterTable`  
  - `alaHAVlanClusterId`  
  - `alaHAVlanClusterIfIndex`  
  - `alaHAVlanClusterInetAddressType`  
  - `alaHAVlanClusterInetAddress`  
  - `alaHAVlanClusterMacAddressType`  
  - `alaHAVlanClusterMacAddress`  
  - `alaHAVlanClusterMulticastStatus`  
  - `alaHAVlanClusterMulticastInetAddressType`  
  - `alaHAVlanClusterMulticastInetAddress`  
  - `alaHAVlanClusterRowStatus`
server-cluster igmp mode

Configures the IGMP mode status for specified cluster.

`server-cluster cluster_id igmp-mode {enable | disable}`

**Syntax Definitions**

- **cluster_id**: The numerical identifier of an existing server cluster.
- **enable**: Enables IGMP mode for cluster ports.
- **disable**: Disables IGMP mode for cluster ports.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The cluster ID specified with this command must already exist in the switch configuration.
- When the IGMP mode is enabled for the cluster, the port list is dynamically learned using the IGMP protocol for the configured IP multicast address.
- For HA VLAN IGMP to work, IGMP must be enabled globally on the switch using the command `ip multicast admin-state enable` command.

**Examples**

- `-> server-cluster 4 igmp-mode enable`
- `-> server-cluster 4 igmp-mode disable`

**Release History**

Release 7.2.1; command was introduced.

**Related Commands**

- `server-cluster ip`: Configures the specified IP, ARP entry to a given cluster.
- `show server-cluster`: Displays the clusters configured in the system.
MIB Objects
alaHAVlanClusterTable
  alaHAVlanClusterId
  alaHAVlanClusterIfIndex
  alaHAVlanClusterInetAddressType
  alaHAVlanClusterInetAddress
  alaHAVlanClusterMacAddressType
  alaHAVlanClusterMacAddress
  alaHAVlanClusterMulticastStatus
  alaHAVlanClusterMulticastInetAddressType
  alaHAVlanClusterMulticastInetAddress
  alaHAVlanClusterRowStatus
**server-cluster ip-multicast**

Configures a multicast IP address for the specified cluster. This command configures an IP multicast address for an L3 cluster.

`server-cluster cluster_id ip-multicast ipm_address`

---

**Syntax Definitions**

- `cluster_id`  
  The numerical identifier of an existing server cluster.

- `ipm_address`  
  The multicast IP address to assign to the cluster.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The cluster ID specified with this command must already exist in the switch configuration.

- A cluster can be assigned an IP address an ARP entry MAC address. Each cluster should have a unique IP-address. IP address is configurable only for L3 clusters.

- Cluster parameters like IP, multicast IP and MAC address can be modified only when the cluster admin status is disabled.

**Examples**

- `-> server-cluster 2 ip-multicast 226.0.0.12`
- `-> server-cluster 4 ip-multicast 226.0.0.14`

**Release History**

Release 7.2.1; command was introduced.

**Related Commands**

- `server-cluster`  
  Configures cluster parameters to create or modify a cluster ID.

- `show server-cluster`  
  Displays the clusters configured in the system.
**MIB Objects**

`alaHAVlanClusterTable`  
`alaHAVlanClusterId`  
`alaHAVlanClusterIfIndex`  
`alaHAVlanClusterInetAddressType`  
`alaHAVlanClusterInetAddress`  
`alaHAVlanClusterMacAddressType`  
`alaHAVlanClusterMacAddress`  
`alaHAVlanClusterMulticastStatus`  
`alaHAVlanClusterMulticastInetAddressType`  
`alaHAVlanClusterMulticastInetAddress`  
`alaHAVlanClusterRowStatus`
server-cluster port

Configures a port assignment for the port list of the specified cluster.

```
server-cluster cluster_id port {chassis/slot/port[-port2] | all}
no server-cluster cluster_id port {chassis/slot/port[-port2] | all}
```

**Syntax Definitions**

- `cluster_id` The numerical identifier of an existing server cluster.
- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number to assign to the cluster port list. Use a hyphen to specify a range of ports (1/15-20).
- `all` Assigns all of the ports that belong to the associated VLAN and NOT all ports on the NI. This parameter applies only to L3 clusters.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8C32E/T24C2/32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a port from the specified cluster port list.
- The cluster ID specified with this command must already exist in the switch configuration.
- Using a port list is not valid for a cluster operating with IGMP mode enabled.
- The `all` parameter does not apply to L2 clusters.

**Examples**

```
-> server-cluster 1 port 1/1/21
-> server-cluster 2 port 1/1/21-23
-> server-cluster 5 port all
-> no server-cluster 1 port 1/1/21
-> no server-cluster 2 port 1/1/21-23
-> no server-cluster 3 port all
```
**Release History**
Release 7.2.1; command was introduced.

**Related Commands**

- **server-cluster**: Configures cluster parameters to create or modify a cluster ID.
- **show server-cluster**: Displays the clusters configured in the system.
- **show mac-learning**: Displays Source Learning MAC Address table information.
- **show vlan**: Displays a list of existing VLANs.
- **show vlan members**: Displays VLAN port assignments.

**MIB Objects**

- **alaHAVlanClusterPortTable**
  - **alaHAVlanClusterId**
  - **alaHAVlanClusterPortIfIndex**
  - **alaHAVlanClusterPortRowStatus**
server-cluster linkagg

Configures a link aggregate assignment for the port list of the specified cluster.

server-cluster cluster_id linkagg agg_id[-agg_id2]

no server-cluster cluster_id linkagg agg_id[-agg_id2]}

Syntax Definitions

cluster_id

agg_id[-agg_id2] The numerical identifier of an existing server cluster.
The link aggregate ID number to assign to the cluster port list. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove a link aggregate ID from the specified cluster port list.
- The cluster ID and link aggregate ID specified with this command must already exist in the switch configuration.
- Using a port list is not valid for a cluster operating with IGMP mode enabled.

Examples

- server-cluster 3 linkagg 1
- server-cluster 4 linkagg 1-3
- no server-cluster 3 linkagg 1

Release History

Release 7.2.1; command was introduced.
Related Commands

- **server-cluster**: Configures cluster parameters to create or modify a cluster ID.
- **show server-cluster**: Displays the clusters configured in the system.
- **show mac-learning**: Displays Source Learning MAC Address table information.
- **show vlan**: Displays a list of existing VLANs.
- **show vlan members**: Displays VLAN port assignments.

MIB Objects

- alaHAVlanClusterPortTable
- alaHAVlanClusterId
- alaHAVlanClusterPortIfIndex
- alaHAVlanClusterPortRowStatus
show server-cluster

Displays the cluster configuration information for the switch.

show server-cluster [cluster_id [port]]

Syntax Definitions

cluster_id The numerical identifier of an existing server cluster.
port Displays the ports and/or link aggregates assigned to a specific cluster.

Defaults

Displays a list of all server clusters configured for the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6880</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specify a cluster ID with this command to display information for a single cluster.
- Use the port parameter with the cluster_id parameter to display information about the ports assigned to the specified cluster.
- An asterisk (*) is displayed to indicate invalid cases, as shown in the command example.

Examples

```
-> show server-cluster
Legend: * = operational state: disabled
Cluster Id Mode Vlan Mac Address Ip Address IGMP Address Loopback Status Name
----------------------------------------------------------------------------------------------------------------------------------------
  * 10 L2 100 01:10:11:22:33:44 - - N/A c-1
  11 L2 100 01:10:11:22:33:44 - - N/A c-2
  12 L2 100 01:10:11:22:33:44 - - N/A -
  13 L3 - 01:12:11:22:33:44 10.135.33.203 - Disabled -
  * 14 L3 - 01:12:11:22:33:45 10.135.33.203 - Disabled -
  15 L3 - 01:00:6e:00:00:44 10.135.33.203 225.0.1.2 Disabled c3igmp

-> show server-cluster 10 port
Legend: * = not valid
Cluster ID Port Port Type
-----------------------------------------------------------------------------
  * 10 1/1/3 Static
  10 1/1/21 Static
```
* 10  0/2  Static
-> show server-cluster 11 port
Legend: * = not valid
Cluster ID  Port    Port Type
----------+-------+--------------
10        1/1/3 Dynamic
10        1/1/21 Dynamic
10        0/2  Dynamic

output definitions

<table>
<thead>
<tr>
<th>Cluster Id</th>
<th>The numerical identifier of a cluster.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Displays the cluster mode as L2 or L3.</td>
</tr>
<tr>
<td>Vlan</td>
<td>Displays the VLAN identifier of the cluster.</td>
</tr>
<tr>
<td>MAC-Address</td>
<td>The MAC address associated with the cluster.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address associated with the cluster.</td>
</tr>
<tr>
<td>IGMP Address</td>
<td>The IGMP address associated with the cluster.</td>
</tr>
<tr>
<td>Loopback Status</td>
<td>The status of Loopback for the cluster, Enabled or Disabled.</td>
</tr>
<tr>
<td>Name</td>
<td>The name representing the cluster.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the port list of the cluster.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Displays the port type, Static or Dynamic.</td>
</tr>
</tbody>
</table>

-> show server-cluster 10
Cluster Id   : 10,
Cluster Name : c-1,
Cluster Mode : L2,
Cluster Vlan : 100,
Cluster Mac-Address: 01:10:11:22:33:44,
Administrative State: Enabled,
Operational State: Disabled,
Operational Flag: VPA is not forwarding

-> show server-cluster 15
Cluster Id   : 15,
Cluster Name : c3igmp,
Cluster Mode : L3,
Cluster IP   : 10.135.33.203,
Cluster Mac-Address: 01:00:6e:00:00:44,
Cluster Mac Type: Dynamic,
IGMP-Mode    : Enabled,
Cluster Multicast IP: 225.0.1.2,
Loopback Status: Disabled,
Administrative State: Enabled,
Operational State: Disabled,
Operational Flag: No IGMP reports received

output definitions

<table>
<thead>
<tr>
<th>Cluster ID</th>
<th>The numerical identifier of a cluster.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Name</td>
<td>The name representing the cluster.</td>
</tr>
<tr>
<td>Cluster Mode</td>
<td>Displays the cluster mode as L2 or L3.</td>
</tr>
<tr>
<td>Cluster IP</td>
<td>The IP address associated with the cluster.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Clusters Mac-Address</th>
<th>The MAC address associated with the cluster.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Mac Type</td>
<td>The type of cluster, Static or Dynamic.</td>
</tr>
<tr>
<td>IGMP-mode</td>
<td>Specifies the status of IGMP-mode, Enabled or Disabled.</td>
</tr>
<tr>
<td>Cluster Multicast IP</td>
<td>The multicast IP address associated with the cluster.</td>
</tr>
<tr>
<td>Loopback Status</td>
<td>The status of Loopback for the cluster, Enabled or Disabled.</td>
</tr>
<tr>
<td>Administrative State</td>
<td>Specifies the administrative status of the cluster, Enabled or Disabled.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Specifies the operational status of the cluster, Enabled or Disabled.</td>
</tr>
<tr>
<td>Operational Flag</td>
<td>Specifies the reason the cluster is operationally down.</td>
</tr>
</tbody>
</table>

Release History

Release 7.2.1; command was introduced.

Related Commands

- `show mac-learning` Displays Source Learning MAC Address Table information.
- `show vlan` Displays a list of existing VLANs.
- `show vlan members` Displays VLAN port assignments.

MIB Objects

alaHAVlanClusterPortTable
  alaHAVlanClusterPortId
  alaHAVlanClusterPortIfIndex
  alaHAVlanClusterPortRowStatus

alaHAVlanClusterTable
  alaHAVlanClusterId
  alaHAVlanClusterInetAddress
  alaHAVlanClusterMacAddressType
  alaHAVlanClusterMacAddress
  alaHAVlanClusterMulticastStatus
  alaHAVlanClusterMulticastInetAddress
  alaHAVlanClusterVlan
  alaHAVlanClusterName
  alaHAVlanClusterAdminStatus
  alaHAVlanClusterMode
  alaHAVlanClusterOperStatus
  alaHAVlanClusterOperStatusFlag
  alaHAVlanClusterLoopback
The VLAN Stacking feature provides a method for tunneling multiple customer VLANs (CVLAN) through a service provider network using one or more service provider VLANs by way of 802.1Q double tagging or VLAN Translation. This feature enables service providers to provide their customers with Transparent LAN Services (TLS). This service is multipoint in nature to support multiple customer sites or networks distributed over the edges of a service provider network.

MIB information for the VLAN Stacking commands is as follows:

- **Filename:** ALCATEL-IND1-E-SERVICE-MIB.mib
- **Module:** alcatelIND1EServiceMIB

- **Filename:** ALCATEL-IND1-VLAN-MGR-MIB.mib
- **Module:** alcatelIND1VLANManagerMIB
A summary of the available commands is listed here:

| VLAN Stacking Service Mode | ethernet-service svlan  
|                           | ethernet-service service-name 
|                           | ethernet-service nni 
|                           | ethernet-service svlan nni 
|                           | ethernet-service sap 
|                           | ethernet-service sap uni 
|                           | ethernet-service sap cvlan 
|                           | ethernet-service sap-profile 
|                           | ethernet-service sap-profile uni-profile 
|                           | ethernet-service uni-profile 
|                           | ethernet-service uni-profile inbound 802.1ab 
|                           | ethernet-service uni uni-profile 
|                           | ethernet-service custom-L2-protocol 
|                           | ethernet-service uni-profile custom-L2-protocol 
|                           | ethernet-service mac-tunneling 
|                           | ethernet-service svlan mac-tunneling 
|                           | ethernet-service transparent-bridging 
| show ethernet-service vlan | show ethernet-service 
| show ethernet-service sap  | show ethernet-service port 
| show ethernet-service nni  | show ethernet-service nni l2pt-statistics 
| show ethernet-service nni l2pt-statistics | show ethernet-service uni l2pt-statistics 
| clear ethernet-service nni l2pt-statistics | show ethernet-service uni l2pt-statistics 
| show ethernet-service uni l2pt-statistics | clear ethernet-service uni l2pt-statistics 
| show ethernet-service uni-profile | show ethernet-service uni-profile l2pt-statistics 
| show ethernet-service custom-L2-protocol | show ethernet-service uni-profile l2pt-statistics 
| show ethernet-service mac-tunneling | clear ethernet-service uni-profile l2pt-statistics 
| show ethernet-service sap-profile | show ethernet-service sap-profile 

| Wire-rate Hardware Loopback Test | loopback-test 
|                                | show loopback-test 
|                                | clear loopback-test counters |
ethernet-service svlan

Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic.

\[
\text{ethernet-service svlan } \{\text{svlan_id}|-\text{svlan_id2}\} \ [\text{admin-state } \{\text{enable} | \text{disable}\}] \ [\text{name description}]
\]

\[
\text{no ethernet-service svlan } \{\text{svlan_id}|-\text{svlan_id2}\}
\]

**Syntax Definitions**

- **svlan_id|-svlan_id2**: The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).
- **enable**: Enables the SVLAN administrative status.
- **disable**: Disables the SVLAN administrative status, which blocks all ports bound to that SVLAN.
- **description**: An alphanumeric string. Use quotes around the string if the VLAN name contains multiple words with spaces between them (for example, “ALE Engineering”).

**Defaults**

By default, the Spanning Tree status is enabled in both the **per-vlan** and **flat** mode when the SVLAN is created.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>description</td>
<td>VLAN ID number</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete an SVLAN or a range of SVLANs. Note that SVLAN port associations are also removed when the SVLAN is deleted.
- This command does not work if the **svlan_id** specified already exists as a standard VLAN.

**Note.** Spanning Tree status for an SVLAN only applies to the Spanning Tree topology calculations for the service provider network. This status is not applied to customer VLANs (CVLANs) and does not affect the customer network topology.
Examples

-> ethernet-service svlan 1001-1005 admin-state enable name “Customer ABC”
-> no ethernet-service svlan 1001

Release History

Release 7.1.1; command introduced.

Related Commands

show ethernet-service vlan Displays a list of SVLANs configured from the switch

MIB Objects

vlanTable
  vlanNumber
  vlanDescription
  vlanType
  vlanAdmStatus
  vlanStatus
**ethernet-service service-name**

Creates a VLAN Stacking service and associates the service with an SVLAN. A service can be carried only on a single SVLAN. All traffic within the associated service is carried on the SVLAN.

```
ethernet-service service-name service_name svlan svlan_id
no ethernet-service service-name service_name svlan svlan_id
```

**Syntax Definitions**

- `service_name` The name of the VLAN Stacking service; an alphanumeric string. Use quotes around string if the service name contains multiple words with spaces between them (for example, “ALE Engineering”).

- `svlan_id` The VLAN ID number that identifies an existing SVLAN to associate with the VLAN Stacking service.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a VLAN Stacking service. Note that when a service is removed, the SVLAN association with that service is also removed.

- If the VLAN Stacking service is associated with a Service Access Point (SAP), then remove the SAP associations before attempting to remove the VLAN Stacking service.

- Each VLAN Stacking service is associated with one SVLAN. Specifying an additional VLAN ID for an existing service is not allowed.

**Examples**

```
-> ethernet-service service-name Marketing svlan 10
-> no ethernet-service service-name Marketing svlan 10
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

ethernet-service svlan

Creates an SVLAN for customer traffic, a management VLAN for provider traffic for multicast traffic.

MIB Objects

alaEServiceTable
  alaEServiceID
  alaEServiceSVLAN
  alaEServiceRowStatus
ethernet-service nni

Configures a switch port or link aggregate as a VLAN Stacking Network Network Interface (NNI) and optionally specifies the vendor TPID value and the legacy BPDU processing status for a VLAN Stacking Network Network Interface (NNI).

```
ethernet-service nni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [tpid tpid_value] [[stp | mvrp] legacy-bpdu {enable | disable}]
```

```
no ethernet-service nni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td></td>
</tr>
<tr>
<td>slot/port [-port2]</td>
<td></td>
</tr>
<tr>
<td>agg_id[-agg_id2]</td>
<td></td>
</tr>
<tr>
<td>tpid_value</td>
<td>0x8100</td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>tpid_value</td>
<td>0x8100</td>
</tr>
<tr>
<td>stp legacy-bpdu</td>
<td>disable</td>
</tr>
<tr>
<td>mvrp legacy-bpdu</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to revert the VLAN Stacking NNI port or link aggregate back to a conventional switch port or aggregate.
- When this command is used, the default VLAN for the NNI port is changed to a VLAN reserved by the switch for applications such as VLAN Stacking. The reserved VLAN cannot be configured using standard VLAN management commands.
• An interface configured with any standard VLAN (non-service) and 802.1q VLAN can now be configured as NNI port. This allows NNI ports to configure 802.1q services, QinQ service, and untagged services using the same uplink NNI port.
  – 802.1q VLAN tagging to a NNI interface will not be allowed if the interface is set with TPID other than 0x8100.
  – The TPID (other than 0x8100) of a NNI interface cannot be modified if the interface is already a tagged member of a legacy VLAN.
  – The binding of service VLAN to a NNI interface is allowed even if the NNI interface is already untagged or tagged with the standard VLAN.

• Enable legacy BPDU support only on VLAN Stacking network ports that are connected to legacy BPDU switches. Enabling legacy BPDU between AOS switches can cause flooding or an unstable network.

• If legacy BPDU is enabled on a network port while at same time BPDU flooding is enabled on user ports, make sure that tagged customer BPDUs are not interpreted by intermediate switches in the provider network.

• Note that if the peer switch connected to the VLAN Stacking network port supports the Provider MAC address (STP, 802.1ad/D6.0 MAC), then enabling legacy BPDU support is not required on the network port. Refer to the following table to determine the type of STP MAC used:

<table>
<thead>
<tr>
<th>STP</th>
<th>Customer MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>{0x01, 0x80, 0xc2, 0x00, 0x00, 0x00}</td>
</tr>
<tr>
<td>Provider MAC address (802.1ad/D6.0)</td>
<td>{0x01, 0x80, 0xc2, 0x00, 0x00, 0x08}</td>
</tr>
<tr>
<td>Provider MAC address (Legacy MAC)</td>
<td>{0x01, 0x80, 0xc2, 0x00, 0x00, 0x00}</td>
</tr>
</tbody>
</table>

• STP legacy BPDU are supported only when the flat Spanning Tree mode is active on the switch.

Examples

-> ethernet-service 10 nni port 1/1/3-5
-> ethernet-service 255 nni port 1/2/1-5 tpid 88a8
-> ethernet-service 500 nni port 1/1/3-5 stp legacy-bpdu enable
-> no ethernet-service 10 nni port 1/1/3
-> no ethernet-service 255 nni linkagg 12-15

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service svlan nni Associates a switch port or link aggregate with a SVLAN.

MIB Objects

alaEServicePortTable
  alaEServicePortID
  alaEServicePortType
  alaEServicePortVendorTpid
  alaEServicePortLegacyStpBpdu
alaEServicePortRowStatus
ethernet-service svlan nni

Associates an NNI port with an SVLAN. A network port connects to another provider bridge and carries both customer and provider traffic.

```plaintext
ethernet-service svlan {svlan_id[svlan_id2]} nni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}

no ethernet-service svlan {svlan_id[svlan_id2]} nni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- **svlan_id[svlan_id2]**: The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).
- **chassis**: The chassis identifier.
- **slot/port [-port2]**: The slot and port number (3/1) of an NNI port. Use a hyphen to specify a range of ports (3/1-5).
- **agg_id[-agg_id2]**: The link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (5-10).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an association between an NNI port and an SVLAN.
- Only SVLAN IDs are accepted with this command. This SVLAN ID specified must already exist in the switch configuration.
- This command only applies to ports or link aggregates configured as VLAN Stacking NNI ports.
- NNI ports can be associated with normal VLANs. This allows NNI ports to carry regular 802.1q tagged traffic as well as SVLAN tagged traffic, and untagged traffic.

**Examples**

- `-> ethernet-service svlan 10 nni port 1/1/3`
- `-> ethernet-service svlan 255 nni port 1/2/1-5`
- `-> ethernet-service svlan 500 nni linkagg 31-35`
-> no ethernet-service svlan 10 nni port 1/1/3
-> no ethernet-service svlan 255 nni port 1/2/5

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **ethernet-service svlan** Creates an SVLAN for tunneling customer traffic.
- **ethernet-service nni** Configures a switch port or link aggregate as a VLAN Stacking NNI.

**MIB Objects**

alaEServiceNniSvlanTable
  alaEServiceNniSvlanNni
  alaEServiceNniSvlanSvlan
  alaEServiceNniSvlanRowStatus
**ethernet-service sap**

Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking service.

```
ethernet-service sap sap_id service-name service_name
```

```
no ethernet-service sap sap_id
```

**Syntax Definitions**

- `sap_id` The SAP ID number identifying the service instance.
- `service_name` The name of the service to associate with this SAP.

**Defaults**

The “default-sap-profile” profile is automatically associated with the SAP ID when the SAP is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete a VLAN Stacking SAP. When a SAP is deleted, all port and CVLAN associations with the SAP are also deleted.
- The service name specified with this command must already exist in the switch configuration. Use the `ethernet-service service-name` command to create a service to associate with the SAP.
- Each SAP ID is associated with only one service; however, it is possible to associate one service with multiple SAP IDs.

**Examples**

```
-> ethernet-service sap 10 service-name CustomerA
```

```
-> no ethernet-service sap 11
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **ethernet-service service-name**  Creates a VLAN Stacking service and associates the service with an SVLAN.
- **ethernet-service sap-profile**  Creates a VLAN Stacking SAP profile.
- **ethernet-service sap sap-profile**  Associates a SAP profile with a SAP ID.

MIB Objects

alaEServiceSapTable
   alaEServiceSapID
   alaEServiceSapServiceID
   alaEServiceSapProfile
   alaEServiceSapRowStatus
**ethernet-service sap uni**

Configures the switch port as a VLAN Stacking User Network Interface (UNI) and associates the port with a VLAN Stacking Service Access Point (SAP). A UNI port is a customer facing port on which traffic enters the SAP.

```
ethernet-service sap sap_id uni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
no ethernet-service sap sap_id uni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- `sap_id` The SAP ID number identifying the service instance.
- `chassis` The chassis identifier.
- `slot/port [-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
- `agg_id[-agg_id2]` The link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (5-10).

**Defaults**

A switch port or a link aggregate becomes a VLAN Stacking UNI port by default when the port or link aggregate is associated with a VLAN Stacking SAP.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an association between a UNI port and a SAP. Note that when the last SAP association is removed, the UNI port converts back to a conventional switch port.
- Only fixed ports can be configured as UNI ports.
- The SAP ID specified with this command must already exist. Use the `ethernet-service sap` command to create a SAP.
- When this command is used, the default VLAN for the UNI port is changed to a reserved VLAN and all customer traffic received is dropped until the type of traffic for the port is configured using the `ethernet-service sap cvlan` command.

**Examples**

```
-> ethernet-service sap 10 uni port 1/1/3
```
-> ethernet-service sap 10 uni port 1/2/1-5
-> ethernet-service sap 10 uni linkagg 31-40
-> no ethernet-service sap 10 uni port 1/2/1-5
-> no ethernet-service sap 10 uni linkagg 31

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **ethernet-service sap** Creates a VLAN Stacking SAP and associates the SAP with a VLAN Stacking SAP profile and service.
- **ethernet-service uni-profile** Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
- **ethernet-service uni uni-profile** Associates a VLAN Stacking UNI profile with a UNI port.

**MIB Objects**

- `alaEServiceSapUniTable`  
  - `alaEServiceSapUniSap`  
  - `alaEServiceSapUniUni`  
  - `alaEServiceSapUniRowStatus`
**ethernet-service sap cvlan**

Associates customer VLAN (CVLAN) traffic with a VLAN Stacking Service Access Point (SAP). The parameter values configured with this command are applied to frames received on all SAP UNI ports and determines the type of customer traffic that is accepted on the UNI ports and processed by the service.

```
ethernet-service sap sap_id cvlan {all | cvlan_id[-cvlan_id2] | untagged}

no ethernet-service sap sap_id cvlan {all | cvlan_id[-cvlan_id2] | untagged}
```

### Syntax Definitions

- **sap_id**: The SAP ID number.
- **all**: Applies the SAP profile to tagged and untagged frames.
- **cvlan_id[-cvlan_id2]**: Applies the SAP profile to frames tagged with the specified CVLAN ID. Use a hyphen to specify a range of CVLAN IDs (for example, 10-12 applies the SAP profile to frames tagged with CVLAN 10, 11, or 12).
- **untagged**: Applies the SAP profile only to untagged frames.

### Defaults

By default, no CVLAN traffic is associated with the SAP ID when the SAP is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove a CVLAN ID or the designation for **all** or **untagged** frames from the SAP. Note that when the last CVLAN parameter is deleted from an SAP configuration, the SAP is not automatically deleted.
- The **all** and **untagged** parameters are configurable in combination with a CVLAN ID. For example, if **untagged** and a CVLAN ID are associated with the same SAP ID, then the SAP profile is applied to only untagged traffic and traffic tagged with the specified CVLAN ID. All other traffic is dropped.
- The SAP ID specified with this command must already exist. Use the **ethernet-service sap** command to create a SAP.
- Configuring the **all** and **untagged** parameters for the same SAP is not allowed. Specify only one of these two parameters per SAP.
• Either the **all** or **untagged** parameters can be configured for the SAP. In such an instance, the default VLAN for the UNI ports associated with the SAP is changed to the VLAN assigned to the SAP related service.

• Only one SAP, with the **all** or **untagged** option, is allowed per UNI. For example, if UNI port 1/17 is part of SAP 10 and SAP 20 and SAP 10 is configured for **all** traffic, then only **untagged** parameter or a CVLAN ID is allowed for SAP 20.

• If you do not specify **all** or **untagged** options with a UNI, then the default VLAN 4095 is set for the UNI and all untagged, untagged control traffic and unmatched tag traffic is dropped.

**Examples**

```plaintext
-> ethernet-service sap 10 cvlan 200  
-> ethernet-service sap 10 cvlan all  
-> ethernet-service sap 11 cvlan 100-150  
-> ethernet-service sap 11 cvlan untagged  
-> no ethernet-service sap 10 cvlan 200  
-> no ethernet-service sap 10 cvlan all  
-> no ethernet-service sap 10 cvlan 100-150  
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**ethernet-service sap**  
Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking service.

**MIB Objects**

alaEServiceSapCvlanTable  
alaEServiceSapCvlanSapId  
alaEServiceSapCvlanCvlan  
alaEServiceSapCvlanMapType  
alaEServiceSapRowStatus
**ethernet-service sap-profile**

Creates a profile for a VLAN Stacking Service Access Point (SAP). Profile attributes are used to define traffic engineering policies that are applied to traffic serviced by the SAP.

```
ethernet-service sap-profile sap_profile_name [bandwidth not-assigned] [[shared | not-shared] ingress-bandwidth mbps] [cvlan-tag {preserve | translate}] priority [not-assigned | map-inner-to-outer-p | map-dscp-to-outer-p | fixed value] [egress-bandwidth mbps]
```

```
no ethernet-service sap-profile sap_profile_name
```

**Syntax Definitions**

- **sap_profile_name**
  - An alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

- **bandwidth not-assigned**
  - Specifies that the SAP profile does not allocate switch resources to enforce bandwidth requirements. Applies only when the profile specifies the default ingress bandwidth value (zero).

- **shared**
  - Shares the ingress bandwidth limit across all SAP ports and CVLANs.

- **not shared**
  - Applies the ingress bandwidth limit to individual SAP ports and CVLANs; bandwidth is not shared.

- **ingress bandwidth mbps**
  - The maximum amount of bandwidth to be allowed for SAP ports, for the incoming traffic, in megabits per second. This parameter can be used only along with the shared option or not-shared option.

- **preserve**
  - Retains the customer VLAN ID (inner tag) and double tags the frame with the SVLAN ID (outer tag).

- **translate**
  - Replaces the customer VLAN ID with the SVLAN ID.

- **priority not-assigned**
  - Specifies that the SAP profile is not assigned with a priority value or priority mapping.

- **map-inner-to-outer-p**
  - Maps the customer VLAN (inner tag) priority bit value to the SVLAN (outer tag) priority bit value.

- **map-dscp-to-outer-p**
  - Maps the customer VLAN (inner tag) DSCP value to the SVLAN (outer tag) priority bit value.

- **fixed value**
  - Sets the SVLAN (outer tag) priority bit to the specified value.

- **egress-bandwidth mbps**
  - The maximum amount of bandwidth to be allowed for SAP ports, for the outgoing traffic, in megabits per second. *This parameter is not supported on an OmniSwitch 6900.*
ethernet-service sap-profile

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>shared</td>
<td>not shared</td>
</tr>
<tr>
<td>mbps</td>
<td>0</td>
</tr>
<tr>
<td>preserve</td>
<td>translate</td>
</tr>
<tr>
<td>not-assigned</td>
<td>map-inner-to-outer-p</td>
</tr>
<tr>
<td>fixed value</td>
<td></td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to delete a SAP profile.
- If a profile is not specified when a SAP is created, a default profile (default-sap-profile) is automatically associated with the SAP.
- Use the ethernet-service sap sap-profile command to associate a profile to a VLAN Stacking SAP.
- Only one SAP profile name is associated with each SAP ID; however, it is possible to associate the same SAP profile name to multiple SAP IDs.
- Configure the ingress-bandwidth or egress-bandwidth parameters to define rate limiting values for the SAP.

Examples

- ethernet-service sap-profile video1 egress-bandwidth 10 cvlan-tag translate priority map-inner-to-outer-p
- ethernet-service sap-profile voice1 not-shared ingress-bandwidth 10 cvlan-tag preserve
- ethernet-service sap-profile voice2 shared ingress-bandwidth 10
- no ethernet-service sap-profile video1

Release History

Release 7.1.1; command introduced.
Related Commands

ethernet-service sap  Creates a VLAN Stacking SAP and associates the SAP with a service.
ethernet-service sap sap-profile  Associates a SAP profile with a SAP ID.
show ethernet-service sap-profile  Displays the profile attribute configuration for a SAP profile.

MIB Objects

alaEServiceSapProfileTable
alaEServiceSapProfileID
alaEServiceSapProfileCvLANTreatment
alaEServiceSapProfileIngressBW
alaEServiceSapProfileEgressBW
alaEServiceSapProfilePriorityMapMode
alaEServiceSapProfileFixedPriority
alaEServiceSapProfileBandwidthShare
alaEServiceSapRowStatus
ethernet-service sap sap-profile

Associates a VLAN Stacking Service Access Point (SAP) with a SAP profile. This command is also used to change an existing SAP profile association.

```
ethernet-service sap sap_id sap-profile sap_profile_name
no ethernet-service sap sap_id
```

### Syntax Definitions

- **sap_id**: The SAP ID number.
- **sap_profile_name**: The name of the SAP profile to associate with this SAP ID.

### Defaults

The “default-sap-profile” profile is automatically associated with the SAP ID when the SAP is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command along with the SAP ID to remove the SAP profile.
- If a profile association already exists for the specified SAP ID, the current profile is replaced with the profile specified with this command.
- To change the profile associated with the SAP back to the default profile, enter “default-sap-profile” with this command.
- Do not specify a service name; doing so returns an error message. This command is only for associating an existing profile to a VLAN Stacking SAP.

### Examples

```
-> ethernet-service sap 10 sap-profile CustomerC
-> ethernet-service sap 11 sap-profile CustomerD
-> ethernet-service sap 11 sap-profile default-sap-profile
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- `ethernet-service sap` Creates a VLAN Stacking SAP and associates the SAP with a VLAN Stacking SAP profile and service.
- `ethernet-service sap-profile` Creates a VLAN Stacking SAP profile.

**MIB Objects**

- `alaEServiceSapTable`
  - `alaEServiceSapID`
  - `alaEServiceSapProfile`
  - `alaEServiceSapRowStatus`
ethernet-service uni-profile

Creates a User Network Interface (UNI) profile that is used to specify how to process control packets ingressing on UNI ports.

```bash
ethernet-service uni-profile uni_profile_name [tunnel-mac mac_address] [l2-protocol protocol] {peer | discard | tunnel | mac-tunnel}
```

```bash
no ethernet-service uni-profile uni_profile_name
```

**Syntax Definitions**

- `uni_profile_name`: Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).
- `mac_address`: The tunnel MAC address to use when configuring MAC tunneling. This parameter is not supported on the OmniSwitch 6900.
- `protocol`: The protocol to which the specified action is applied. Refer to the table in the “Usage Guidelines” section of this command page for a list of protocol keywords to select.
- `peer`: Allows the UNI port to participate in the specified protocol.
- `discard`: Discards the specified PDU.
- `tunnel`: Tunnels the specified PDU across the provider network.
- `mac-tunnel`: Changes the destination MAC address to either the configured or default tunnel MAC address before forwarding. This parameter is not supported on the OmniSwitch 6900.

**Defaults**

By default, the tunnel MAC address is set to 01:00:0c:cd:cd:d0. Refer to the table in the “Usage Guidelines” section of this command page for the default action settings for each protocol parameter.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete a UNI profile. Remove any UNI profile associations with UNI ports before attempting to modify or delete the profile.
- If a user-configured UNI profile is not associated with a UNI port, then the default profile (`default-uni-profile`) is used to process control packets ingressing on the port.
The following table provides the default and supported profile actions for each protocol parameter:
The `oam`, `lacpmarker`, `udld`, `pagp`, `cdp`, `vtp`, `dtp`, `pvst`, `vlan`, and `uplink` protocol keywords are not supported with this command on the OmniSwitch 6900.

To specify how to process tagged and untagged 802.1AB control frames, use the `ethernet-service uni-profile inbound` command.

Up to five unique UNI profile combinations, including the default and built-in profiles, are allowed per switch.

### Examples

```bash
-> ethernet-service uni-profile uni_1 12-protocol mvrp discard
-> ethernet-service uni-profile uni_2 tunnel-mac 01:00:0c:cd:cd:cd 12-protocol pagp mac-tunnel
-> ethernet-service uni-profile uni_3 12-protocol uplink tunnel
ERROR: Only 5 profiles are allowed for this type
-> no ethernet-service uni-profile uni_1
-> no ethernet-service uni-profile uni_2
```

### Release History

Release 7.1.1; command introduced.
Release 8.6R1; `tunnel-mac` address and protocol parameters added, `mac-tunnel` action parameter added.
Release 8.9R1; Omniswitch 6560 support added.
Related Commands

- `ethernet-service uni-profile custom-L2-protocol` Assigns a custom L2 protocol MAC address entry to a UNI profile.
- `ethernet-service uni uni-profile` Associates a VLAN Stacking UNI profile with a UNI port.
- `ethernet-service sap uni` Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).
- `show ethernet-service uni` Displays the profile associations for VLAN Stacking UNI ports.
- `show ethernet-service uni-profile` Displays the profile attribute configuration for VLAN Stacking UNI profiles.

MIB Objects

- `alaEServiceUNIProfileTable`
  - `alaEServiceUNIProfileID`
  - `alaEServiceUNIProfileStpBpduTreatment`
  - `alaEServiceUNIProfile8021xTreatment`
  - `alaEServiceUNIProfile8023adTreatment`
  - `alaEServiceUNIProfileMvrpTreatment`
  - `alaEServiceUNIProfileAmapTreatment`
  - `alaEServiceUNIProfileVtpTreatment`
  - `alaEServiceUNIProfileVlanTreatment`
  - `alaEServiceUNIProfileUplinkTreatment`
  - `alaEServiceUNIProfileUdldTreatment`
  - `alaEServiceUNIProfilePvstTreatment`
  - `alaEServiceUNIProfilePagpTreatment`
  - `alaEServiceUNIProfileLacpmarkerTreatment`
  - `alaEServiceUNIProfileDtpTreatment`
  - `alaEServiceUNIProfileCdpTreatment`
  - `alaEServiceUNIProfileTunnelMac`
  - `alaEServiceUNIProfileOamTreatment`
  - `alaEServiceUNIProfileRowStatus`
ethernet-service uni-profile inbound 802.1ab

Configures the treatment of Layer 2 tagged and untagged 802.1AB control frames that are received on UNI ports. Use this command to specify a different action (peer, drop, or tunnel) based on the tagged and untagged state of an 802.1AB control frame.

```
ethernet-service uni-profile uni_profile_name inbound {tagged | untagged | both} l2-protocol 802.1ab
{peer | discard | tunnel}
```

```
no ethernet-service uni-profile uni_profile_name
```

**Syntax Definitions**

- `uni_profile_name`  
  Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

- `tagged`  
  The specified action is applied only to tagged 802.1AB control frames.

- `untagged`  
  The specified action is applied only to untagged 802.1AB control frames.

- `both`  
  The specified action is applied to both tagged and untagged 802.1AB control frames.

- `peer`  
  Allows the UNI port to participate in the 802.1AB protocol.

- `discard`  
  Discards 802.1AB PDUs.

- `tunnel`  
  Tunnels 802.1AB PDUs across the provider network.

**Defaults**

By default, tagged and untagged 802.1AB control frames are dropped.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete a UNI profile. Remove any UNI profile associations with UNI ports before attempting to modify or delete the profile.

- When only the `tagged` keyword is used, the specified action is applied to tagged traffic and the default action (`discard`) is applied to untagged traffic.

- When only the `untagged` keyword is used, the specified action is applied to untagged traffic and the default action (`discard`) is applied to tagged traffic.
• Only the **tunnel** and **discard** actions can be configured for tagged control frames.

• Only the **peer** and **discard** actions can be configured for untagged control frames.

• The treatment of 802.1AB control frames received on access ports can either be mixed (different for tagged, different for untagged) or the same for both tagged and untagged control frames. To switch between mixed and the same, set the action for tagged and untagged frames back to the default (**discard**).

• Use the **ethernet-service uni-profile** command to configure the treatment for other protocol control frames. This command applies only to 801.1AB frames.

**Examples**

```
-> ethernet-service uni-profile lldp-tagged inbound tagged l2-protocol 802.1ab tunnel
-> ethernet-service uni-profile lldp-untagged inbound untagged l2-protocol 802.1ab peer
-> ethernet-service uni-profile lldp-diff inbound tagged l2-protocol 802.1ab tunnel inbound untagged l2-protocol 802.1ab peer
-> ethernet-service uni-profile lldp-both inbound both l2-protocol 802.1ab discard
-> no ethernet-service uni-profile lldp-tagged
-> no ethernet-service uni-profile lldp-untagged
-> no ethernet-service uni-profile lldp-diff
-> no ethernet-service uni-profile lldp-both
```

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

**ethernet-service uni-profile**  Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.

**show ethernet-service uni-profile**  Displays the profile attribute configuration for VLAN Stacking UNI profiles.
## MIB Objects

<table>
<thead>
<tr>
<th>Object Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaEServiceUNIProfileTable</td>
</tr>
<tr>
<td>alaEServiceUNIProfileID</td>
</tr>
<tr>
<td>alaEServiceUNIProfileStpBpduTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfile8021xTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfile8021ABTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfile8023adTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileMvrpTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileAmapTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileVtpTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileVlanTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileUplinkTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileVstTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileUdldTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfilePagpTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileLacpmarkerTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileDtpTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileCdpTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileTunnelMac</td>
</tr>
<tr>
<td>alaEServiceUNIProfileOamTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfile8021ABTagTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfile8021ABUnTagTreatment</td>
</tr>
<tr>
<td>alaEServiceUNIProfileRowStatus</td>
</tr>
</tbody>
</table>
ethernet-service uni uni-profile

 Associates a VLAN Stacking User Network Interface (UNI) profile with a UNI port.

 ethernet-service uni {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} uni-profile
 uni_profile_name

 **Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port [-port2]</td>
<td>The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).</td>
</tr>
<tr>
<td>agg_id[-agg_id2]</td>
<td>The link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (5-10).</td>
</tr>
<tr>
<td>uni_profile_name</td>
<td>Alphanumeric string. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).</td>
</tr>
</tbody>
</table>

**Defaults**

The default profile (default-uni-profile) is used to process control packets ingressing on a UNI port. This profile is assigned at the time a port is configured as a VLAN Stacking UNI.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This UNI profile name specified with this command must already exist in the switch configuration.
- To change the profile associated with a UNI port, use this command and specify a different profile name than the one currently associated with the port. The last profile associated with the port, is the profile that is applied to UNI port traffic.
- To change the profile associated with a UNI port back to the default profile, enter “default-uni-profile” with this command.
- On the OmniSwitch 6465, OmniSwitch 6860, OmniSwitch 6860N, and OmniSwitch 6865, there are also two built-in UNI profiles (ieee-fwd-all and ieee-drop-all) that can be assigned to a UNI port. Use one of the profiles to tunnel or discard all IEEE multicast MAC address traffic received on the UNI port.
  - When a UNI port is assigned to the ieee-fwd-all profile, all L2 protocol control packets destined for 01:80:C2:00:00:XX are forwarded as normal data. However, control packets with a destination MAC address of 01:80:C2:00:00:01, 01:80:C2:00:00:04, or 01:80:C2:00:00:08 are not forwarded.
VLAN Stacking Commands

end-to-end.

- When a UNI port is assigned to the `ieee-drop-all` profile, all L2 protocol control packets destined for 01:80:C2:00:00:XX are discarded.
- When a UNI port is assigned to either one of the built-in profiles (`ieee-fwd-all` or `ieee-drop-all`), tunneled L2 protocol control packets (tagged packets with SVLAN ID) received on NNI ports are forwarded as normal data.

**Examples**

```bash
-> ethernet-service uni port 1/1/3 uni-profile uni_1
-> ethernet-service uni linkagg 1-5 uni-profile uni_2
-> ethernet-service uni port 1/2/1-5 uni-profile default-uni-profile
-> ethernet-service uni port 1/1/6 uni-profile ieee-fwd-all
-> ethernet-service uni port 1/1/7 uni-profile ieee-drop-all
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `ethernet-service uni-profile` Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
- `ethernet-service sap uni` Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).

**MIB Objects**

- `alaEServicePortTable`
  - `alaEServicePortID`
  - `alaEServicePortType`
  - `alaEServicePortUniProfile`
  - `alaEServiceSapUniRowStatus`
**ethernet-service custom-L2-protocol**

Creates a custom L2 protocol MAC address entry with an optional mask, EtherType, or SSAP/DSAP protocol identifier. A custom L2 protocol entry is configured for a proprietary protocol with a destination multicast MAC address and is assigned to a UNI profile for specific packet control.

```
ethernet-service custom-L2-protocol custom_protocol_name mac mac_address [mask mask | ethertype ethertype [subtype subtype] | ssap/dsap ssap/dsap pid pid]
no ethernet-service custom-L2-protocol name
```

**Syntax Definitions**

- `custom_protocol_name`: An alphanumeric string (up to 32 characters) that identifies the custom L2 protocol entry.
- `mac_address`: A multicast MAC address for the custom L2 protocol entry (for example, 01:80:c2:00:11:11).
- `mask`: A mask defines a range of MAC addresses for the custom L2 protocol MAC address entry (for example, ff:ff:ff:ff:00).
- `ethertype`: An integer value to specify a generic EtherType.
- `subtype`: An integer value to specify a Sub-Type for the EtherType.
- `ssap/dsap`: Source service access point and destination service access point specific to LLC/SNAP in numerical or hexadecimal format.
- `pid`: Protocol identifier.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the configured custom L2 protocol entry. A custom L2 protocol entry cannot be deleted if the entry is assigned to a UNI profile that is assigned to a UNI port.
- Consider the following command guidelines when configuring a custom L2 protocol:
When configuring a custom L2 protocol with ...

<table>
<thead>
<tr>
<th>The ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>a MAC address and no mask</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>a MAC address with a mask</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>an EtherType and optional Sub-Type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>an optional SSAP/DSAP and PID</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- The MAC address, mask, EtherType, Sub-Type, SSAP/DSAP, and PID cannot be modified once the custom L2 protocol is created. The custom L2 protocol must be deleted and created again with the new values required.
- A custom L2 protocol is assigned to an existing UNI L2 protocol profile using the **ethernet-service uni-profile custom-L2-protocol** command. The action for the custom L2 protocol entry is specified when the entry is assigned to a UNI L2 protocol profile.

**Examples**

- `-> ethernet-service custom-L2-protocol tunnel-mac mac 01:80:c2:00:11:11`
- `-> ethernet-service custom-L2-protocol tunnel-mac-range mac 01:80:c2:00:11:11 mask ff:ff:ff:ff:ff:00`
- `-> ethernet-service custom-L2-protocol tunnel-mac-ethertype mac 01:80:c2:00:11:11 ethertype 0x5555`
- `-> ethernet-service custom-L2-protocol tunnel-mac-ethersubtype mac 01:80:c2:00:11:11 ethertype 0x5556 subtype 120`
- `-> ethernet-service custom-L2-protocol tunnel-mac-ssap mac 01:80:c2:00:11:11 ssap/dsap 43/43 pid 3`
- `-> ethernet-service custom-L2-protocol discard-mac-range mac 01:80:c2:00:11:11 mask ff:ff:ff:00:ff:ff`

**Release History**

Release 8.6R1; command introduced.
Release 8.9R1; Omniswitch 6560 support added.
### Related Commands

- **ethernet-service uni-profile custom-L2-protocol**
  Assigns a custom L2 protocol entry to a UNI profile.

- **show ethernet-service custom-L2-protocol**
  Displays the custom L2 protocol configuration for the switch.

### MIB Objects

- alaEServiceCustomL2ProtocolTable
  - alaEServiceCustomL2ProtocolName
  - alaEServiceCustomL2ProtocolMac
  - alaEServiceCustomL2ProtocolMask
  - alaEServiceCustomL2ProtocolEtherType
  - alaEServiceCustomL2ProtocolEtherSubType
  - alaEServiceCustomL2ProtocolSsap
  - alaEServiceCustomL2ProtocolDsap
  - alaEServiceCustomL2ProtocolId
  - alaEServiceCustomL2ProtocolRowStatus
ethernet-service uni-profile custom-L2-protocol

Assigns a custom L2 protocol entry to a UNI profile.

```
ethernet-service uni-profile uni_profile_name custom-L2-protocol custom_protocol_name {tunnel | discard | mac-tunnel}
```

```
no ethernet-service uni-profile uni_profile_name custom-L2-protocol custom_protocol_name
```

**Syntax Definitions**

- `uni_profile_name` Name of the configured UNI profile.
- `custom_protocol_name` Name of the configured custom L2 protocol entry to assign to the specified UNI profile.
- `tunnel` Tunnels packets with a destination MAC address that matches the MAC address configured for the custom L2 protocol. The MAC address of the packet is not changed.
- `discard` Discards packets with a destination MAC address that matches the MAC address configured for the custom L2 protocol.
- `mac-tunnel` Changes the destination MAC address of a packet to the configured tunnel MAC address for the specified UNI profile.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the custom L2 protocol entry from the UNI profile.
- If the specified UNI profile is already assigned to a UNI port, then a custom L2 protocol entry cannot be assigned or deleted from the UNI profile.
- The `tunnel` and `discard` actions apply to all traffic matching a custom L2 protocol entry.
- The `mac-tunnel` action applies only to traffic matching a custom L2 protocol entry that was configured with an EtherType and optional Sub-Type value or an SSAP/DSAP PID value.
- More than one custom L2 protocol entry can be assigned to a UNI profile, but not in the same command line. Configure each custom L2 protocol assignment one at a time; a separate command for each entry.
Examples

-> ethernet-service uni-profile uni-prof1 custom-L2-protocol tunnel-mac tunnel
-> ethernet-service uni-profile uni-prof2 custom-L2-protocol tunnel-mac-range tunnel
-> ethernet-service uni-profile uni-prof3 custom-L2-protocol tunnel-mac-ethertype mac-tunnel
-> ethernet-service uni-profile uni-prof4 custom-L2-protocol tunnel-mac-ethersubtype tunnel
-> ethernet-service uni-profile uni-prof5 custom-L2-protocol tunnel-mac-ssap mac-tunnel
-> ethernet-service uni-profile uni-prof6 custom-L2-protocol discard-mac-range discard
-> ethernet-service uni-profile uni-prof6 custom-L2-protocol discard-mac-ethertype discard
-> ethernet-service uni-profile uni-prof6 custom-L2-protocol discard-mac-ssap discard
-> ethernet-service uni-profile uni-prof7 custom-L2-protocol tunnel-mac tunnel ERROR: A profile that is bound to a UNI cannot be modified

-> no ethernet-service uni-profile uni-prof1 custom-L2-protocol tunnel-mac-ethertype
-> no ethernet-service uni-profile uni-prof7 custom-l2-protocol tunnel-mac
ERROR: UNI Profile must be unused by any UNI port before disassociation of a Custom L2 Protocol

Release History

Release 8.6R1; command introduced.
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

show ethernet-service uni-profile Displays the UNI profile configuration for the switch, which includes any custom L2 protocol assignments.

MIB Objects

alaEServiceUNIProfileL2CustomProtocolTable
alaEServiceUNIProfileL2CustomProtocolID
alaEServiceUNIProfileL2CustomProtocolID
alaEServiceUNIProfileL2CustomProtocolType
alaEServiceUNIProfileL2CustomProtocolRowStatus
**ethernet-service mac-tunneling**

Configures the global MAC tunneling status. When enabled (the default), MAC tunneling is active for all UNI profile protocols that are configured with the MAC tunneling action.

```plaintext
ethernet-service mac-tunneling {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Globally enables the MAC tunneling status.</td>
</tr>
<tr>
<td>disable</td>
<td>Globally disables the MAC tunneling status.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>6900</th>
<th>X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The status of MAC tunneling can be configured on a global or per-SVLAN basis.
  - When MAC tunneling is enabled globally, the per-SVLAN MAC tunneling configuration is not active.
  - When MAC tunneling is disabled globally, the per-SVLAN MAC tunneling configuration is active.
- Any changes to the global MAC tunneling status requires a switch reload to activate.
- The global tunnel MAC address is set to 01:00:0C:CD:CD:D0 by default, which is the CISCO tunnel MAC address that is used for Generic Bridge PDU Tunneling (GBPT). A different tunnel MAC address can also be configured for a specific UNI profile and will apply only to packets processed by that profile.
- When L2 protocol packets are received on a UNI port and the associated UNI profile for that port is configured with a MAC tunnel action for that protocol, the destination MAC address for the packets is changed to the tunnel MAC address. The packets are then sent out the NNI port associated with the SVLAN.
- When L2 tunneled packets (with a tunnel MAC as the destination address) are received on an NNI port, the tunnel MAC address is replaced with the protocol MAC address. The packets are then forwarded to the respective UNI port associated with the SVLAN.
Examples

-> ethernet-service mac-tunneling disable
INFO :Changed mac-tunnel feature status will take effect if command is saved on next switch reboot
-> ethernet-service mac-tunneling enable

Release History

Release 8.6R1; command introduced.
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

- `ethernet-service svlan mac-tunneling` Configures the MAC tunneling status for an SVLAN.
- `show ethernet-service mac-tunneling` Displays the global status of MAC tunneling for the switch.

MIB Objects

- alaEServiceGlobals
  - alaEServiceGlobalMacTunneling
ethernet-service svlan mac-tunneling

Configures the MAC tunneling status on a per-SVLAN basis. Enabling MAC tunneling for specific SVLANs limits the trapping of GBPT packets for processing to only those SVLANs.

**ethernet-service svlan svid1[-svid2] mac-tunneling {enable | disable}**

---

### Syntax Definitions

**svlan_id[svlan_id2]**

The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).

**enable**

Enables the MAC tunneling status for the specified SVLAN.

**disable**

Disables the MAC tunneling status for the specified SVLAN.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- Enabling MAC tunneling on a per-SVLAN basis or on a global basis is mutually exclusive; make sure MAC tunneling is globally disabled before attempting to enable MAC tunneling for the specified SVLAN.

- When MAC tunneling is enabled globally, all GBPT packets are trapped for processing even if there is no MAC tunneling action configured for the associated UNI profile. This limits the rate at which these packets are forwarded.

- Enabling MAC tunneling for specific SVLANs limits the trapping of GBPT packets to only those SVLANs where it is needed for MAC tunneling; other SVLANs forward the traffic without trapping the GBPT packets.

- Use the **show ethernet-service vlan** command to display the MAC tunneling status for the SVLAN ID.

- A maximum of four SVLANs can have MAC tunneling enabled at the same time.
Examples

-> ethernet-service svlan 1000 mac-tunneling enable
-> ethernet-service svlan 2000-2005 mac-tunneling enable
-> ethernet-service svlan 1000 mac-tunneling disable
-> show ethernet-service vlan 2000

Name : VLAN 2000,
Type : Service Vlan,
Administrative State : enabled,
Operational State : disabled,
IP Router Port : disabled,
IP MTU : 1500
MAC Tunneling : enabled,

Release History

Release 8.6R1; command introduced.
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

ethernet-service mac-tunneling   Configures the global MAC tunneling status.
show ethernet-service vlan      Displays a list of VLANs and their attributes configured on the switch.

MIB Objects

vlanTable
  vlanNumber
  vlanDescription
  vlanMacTunneling
**ethernet-service transparent-bridging**

Configures transparent bridging which associates VLAN Stacking Network Interface (NNI) ports with all VLANs even if they are not created on the switch.

```
ethernet-service transparent-bridging [nni port chassis/slot/port[-port2] | nni linkagg agg_id[-agg_id2] {enable | disable}]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port [-port2]` The slot and port number.
- `agg_id[-agg_id2]` The link aggregate ID.
- `enable` Enables the specified legacy BPDU support.
- `disable` Disables the specified legacy BPDU support.

**Defaults**

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>
```

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Transparent bridging supports both global and port level enable/disable commands.
- Port level configuration is not accepted if transparent bridging is not enabled globally.
- When transparent bridging is disabled globally, the port level transparent bridging configuration is deleted. The port level configuration must be re-configured after re-enabling transparent bridging globally.
- Transparent bridging is only supported on NNI ports and only on NNI ports that are configured with at least one SVLAN.
- Transparent bridging can only be configured when STP is set to operate in flat mode; it is not supported when the STP is set to operate in MSTP mode.
- Dual-homed Link (DHL) and transparent bridging are not supported on the same NNI port.
Examples

-> ethernet-service transparent-bridging enable
-> ethernet-service nni port 1/1/5 transparent-bridging enable
-> ethernet-service nni linkagg 5 transparent-bridging enable

Release History

Release 8.3.1; command introduced.

Related Commands

show ethernet-service       Displays configuration information for VLAN Stacking Ethernet services.
show ethernet-service nni   Displays configuration information for NNI ports

MIB Objects

alaEServiceGlobals
  alaEServiceGlobalMacTunneling
alaEServicePortTable
  alaEServicePortID
  alaEServicePortType
  alaEServicePortTransBridging
  alaEServicePortRowStatus
show ethernet-service vlan

Displays a list of VLANs configured on the switch. Use this command to identify VLAN Stacking SVLANs.

show ethernet-service vlan [vlan_id-2]

Syntax Definitions

- vlan_id-[vlan_id2] The VLAN ID number identifying the SVLAN. Use a hyphen to specify a range of VLAN IDs (10-12).

Defaults

By default, all VLANs are displayed if a VLAN or range of VLANs is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify a single VLAN ID or a range of VLAN IDs to display configuration information for the specific VLANs.

Examples

```bash
-> show ethernet-service vlan
vlan    type   admin   oper   ip    mtu          name
-------+--------+-------+-------+------+------+------------------
1      std    Ena     Ena   1500    VLAN 1
200    std    Ena     Dis   1500    VLAN 200
300    std    Ena     Dis   1500    VLAN 300
400    router Ena     Ena   1500    ROUTER VLAN 400
500    router Ena     Dis   1500    ROUTER VLAN 500
777    std    Ena     Dis   1500    VLAN 777
800    vstk   Ena     Dis   1500    VLAN 800
1000   vstk   Ena     Dis   1500    VLAN 1000
1001   vstk   Ena     Dis   1500    VLAN 1001
1002   vstk   Ena     Dis   1500    VLAN 1002
1003   vstk   Ena     Dis   1500    VLAN 1003
1004   std    Ena     Dis   1500    VLAN 1004
1005   std    Ena     Dis   1500    VLAN 1005
1006   std    Ena     Dis   1500    VLAN 1006
1007   std    Ena     Dis   1500    VLAN 1007
1008   std    Ena     Dis   1500    VLAN 1008
1009   std    Ena     Dis   1500    VLAN 1009
```
1010 std Ena Dis Dis 1500 VLAN 1010

-> show ethernet-service vlan 1000-1003

<table>
<thead>
<tr>
<th>vlan</th>
<th>type</th>
<th>admin</th>
<th>oper</th>
<th>ip</th>
<th>mtu</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>vstk</td>
<td>Ena</td>
<td>Dis</td>
<td>Dis</td>
<td>1500</td>
<td>VLAN 1000</td>
</tr>
<tr>
<td>1001</td>
<td>vstk</td>
<td>Ena</td>
<td>Dis</td>
<td>Dis</td>
<td>1500</td>
<td>VLAN 1001</td>
</tr>
<tr>
<td>1002</td>
<td>vstk</td>
<td>Ena</td>
<td>Dis</td>
<td>Dis</td>
<td>1500</td>
<td>VLAN 1002</td>
</tr>
<tr>
<td>1003</td>
<td>vstk</td>
<td>Ena</td>
<td>Dis</td>
<td>Dis</td>
<td>1500</td>
<td>VLAN 1003</td>
</tr>
</tbody>
</table>

**output definitions**

- **vlan**: The VLAN ID number identifying the instance.
- **type**: The type of VLAN.
- **admin**: The administrative state of the VLAN. (Ena or Dis).
- **oper**: The operation status of the VLAN (Ena or Dis).
- **ip**: The status of the IP router port (Ena or Dis).
- **mtu**: The IP MTU value configured for the VLAN.
- **name**: The user-defined text description for the VLAN. By default, the VLAN ID is specified for the description.

-> show ethernet-service vlan 1001

**Name**: VLAN 1001,
**Type**: Service Vlan,
**Administrative State**: enabled,
**Operational State**: disabled,
**IP Router Port**: disabled,
**IP MTU**: 1500
**MAC Tunneling**: disabled,

**output definitions**

- **Name**: The user-defined text description for the VLAN. By default, the VLAN ID is specified for the description.
- **Type**: The type of VLAN.
- **Administrative State**: The administrative state of the VLAN (enabled or disabled).
- **Operational State**: The operational status of the VLAN (enabled or disabled).
- **IP Router Port**: The IP router interface status (enabled = IP router interface exists for the VLAN or disabled = no IP router port exists for the VLAN).
- **IP MTU**: The IP MTU value configured for the VLAN.
- **MAC Tunneling**: The MAC tunneling status for the VLAN (enabled or disabled).

**Release History**

Release 7.1.1; command introduced.
Release 8.6R1; “MAC Tunneling” field added.
Related Commands

- **ethernet-service svlan**
  Creates a VLAN Stacking VLAN (SVLAN) for tunneling customer traffic, a management SVLAN for provider traffic application uses to distribute multicast traffic.

- **ethernet-service svlan mac-tunneling**
  Configures the MAC tunneling status on a per-SVLAN basis.

- **show ethernet-service**
  Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

- **vlanTable**
  - **vlanNumber**
  - **vlanDescription**
  - **vlanAdmStatus**
  - **vlanOperStatus**
  - **vlanRouterStatus**
  - **vlanType**
  - **vlanMtu**
  - **vlanMacTunneling**
show ethernet-service

Displays configuration information for VLAN Stacking Ethernet services.

show ethernet-service [service-name service_name | svlan svlan_id | transparent-bridging]

Syntax Definitions

service_name

The name of an existing VLAN Stacking service. Use quotes around string if the service name contains multiple words with spaces between them (for example, “ALE Engineering”).

svlan_id

The VLAN ID number that identifies an existing SVLAN.

transparent-bridging

Display the global status of transparent bridging for the switch.

Defaults

By default, all services are displayed if a service name or SVLAN ID is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Enter the name of a service to display configuration information for a specific service.
- Enter an SVLAN ID to display configuration information for all services that are associated with a specific SVLAN.

Examples

-> show ethernet-service

Service Name : VideoOne
SVLAN : 300
NNI(s) : 1/2/1, 1/2/2
SAP Id : 20
  UNIs : 1/1/1, 1/1/2
  CVLAN(s) : 10, 20
  sap-profile : sap-video1
SAP Id : 30
  UNIs : 1/1/3
  CVLAN(s) : untagged, 40
  sap-profile : sap-video2

Service Name : CustomerABC
VLAN Stacking Commands

SVLAN : 255
NNI(s) : 1/1/22
SAP Id : 10
  UNIs : 1/2/1, 1/2/2
  CVLAN(s) : 500, 600
  sap-profile : default-sap-profile

-> show ethernet-service service-name CustomerABC

Service Name : CustomerABC
  SVLAN : 255
  NNI(s) : 1/1/22
  SAP Id : 10
  UNIs : 1/2/1, 1/2/2
  CVLAN(s) : 500, 600
  sap-profile : default-sap-profile

-> show ethernet-service svlan 300

Service Name : VideoOne
  SVLAN : 300
  NNI(s) : 1/2/1, 1/2/2
  SAP Id : 20
  UNIs : 1/1/1, 1/1/2
  CVLAN(s) : 10, 20
  sap-profile : sap-video1
  SAP Id : 30
  UNIs : 1/1/3
  CVLAN(s) : untagged, 40
  sap-profile : sap-video2

-> show ethernet-service transparent-bridging

Global Transparent Bridging : enabled,

(output definitions)

<table>
<thead>
<tr>
<th>Service Name</th>
<th>The name of the VLAN Stacking service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVLAN</td>
<td>Displays the SVLAN ID associated with the service. Note that SVLAN appears as the field name if the VLAN ID is an SVLAN.</td>
</tr>
<tr>
<td>NNI(s)</td>
<td>VLAN Stacking Network Network Interface ports associated with the service to tunnel SVLAN customer traffic.</td>
</tr>
<tr>
<td>SAP Id</td>
<td>The ID number for the VLAN Stacking Service Access Point that is applied to the service.</td>
</tr>
<tr>
<td>UNIs</td>
<td>VLAN Stacking User Network Interface ports that receive customer traffic.</td>
</tr>
<tr>
<td>CVLAN(s)</td>
<td>Customer VLAN IDs ingressing on UNI ports.</td>
</tr>
<tr>
<td>sap-profile</td>
<td>The name of the SAP profile associated with the SAP.</td>
</tr>
<tr>
<td>Global Transparent Bridging</td>
<td>Displays whether transparent bridging is enabled globally on the switch.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Related Commands

**ethernet-service service-name**  Creates a VLAN Stacking service and associates the service with an SVLAN.

**show ethernet-service vlan**  Displays a list of all or a range of configured SVLANs or the parameters of a specified SVLAN.

**ethernet-service transparent-bridging**  Configures transparent bridging globally or on a port/linkagg.

MIB Objects

alaEServiceTable
    alaEServiceID
    alaEServiceSVLAN
alaEServiceNniSvlanTable
    alaEServiceNniSvlanNni
alaEServiceSapTable
    alaEServiceSapID
alaEServiceSapUniTable
    alaEServiceSapUniUni
alaEServiceSapCvlanTable
    alaEServiceSapCvlanCvlan
    alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
    alaEServiceProfileID
show ethernet-service sap

Displays configuration information for VLAN Stacking Service Access Points (SAP).

show ethernet-services sap [sap_id]

Syntax Definitions

sap_id

The SAP ID number identifying the service instance.

Defaults

By default, all SAPs are displayed if a SAP ID is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6685</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify a single SAP ID to display configuration information for a specific SAP.

Examples

-> show ethernet-services sap

    SAP Id : 10
      UNIs : 1/2/1, 1/2/1
      CVLAN(s) : 500, 600
      sap-profile : default-sap-profile

    SAP Id : 20
      UNIs : 1/1/1, 1/1/2
      CVLAN(s) : 10, 20
      sap-profile : sap-video1

    SAP Id : 30
      UNIs : 1/1/3
      CVLAN(s) : 30, 40
      sap-profile : sap-video2

-> show ethernet-service sap 10

    SAP Id : 10
      UNIs : 1/2/1, 1/2/1
      CVLAN(s) : 500, 600
      sap-profile : default-sap-profile
VLAN Stacking Commands

show ethernet-service sap

output definitions

| SAP Id | The ID number for the VLAN Stacking Service Access Point that is applied to the service. |
| UNIs | VLAN Stacking User Network Interface ports that receive customer traffic. |
| CVLAN(s) | Customer VLAN IDs ingressing on UNI ports. |
| sap-profile | The name of the SAP profile associated with the SAP. |

Release History

Release 7.1.1; command introduced.

Related Commands

ethernet-service sap | Creates a VLAN Stacking Service Access Point (SAP) and associates the SAP with a VLAN Stacking SAP profile and service. |
show ethernet-service | Displays configuration information for VLAN Stacking Ethernet services. |
show ethernet-service sap-profile | Displays the profile attribute configuration for SAP profiles. |

MIB Objects

alaEServiceSapTable
alaEServiceSapProfileTable
alaEServiceSapUnUnTable
alaEServiceSapUniUni
alaEServiceSapCvlanTable
alaEServiceSapCvlanCvlan
alaEServiceSapCvlanMapType
alaEServiceSapProfileID7
show ethernet-service port

Displays configuration information for a VLAN Stacking service port.

show ethernet-service port {chassis/slot/port | linkagg agg_id}

Syntax Definitions

chassis
The chassis identifier.

slot/port
The slot and port number (3/1).

agg_id
The link aggregate ID number.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specifying a slot/port or link aggregate ID number is required with this command.

Examples

-> show ethernet-service port 1/1/10

Interface : 1/1/10
Port Type : UNI
  UNI Profile  : default-uni-profile
  Default SVLAN : 4095
Service Name : svlan_service
  SVLAN  : 20
  NNI(s)  : No NNIs configured
  SAP Id : 1
    UNIs    : 1/1/10
    CVLAN(s) : 200
    sap-profile : translate_profile

-> show ethernet-service port 1/1/22

Interface : 1/1/22
Port Type : NNI
Service Name : CustomerABC
SVLAN   : 255
NNI(s)  : 1/1/22
SAP Id  : 10
   UNIs           : 1/2/1, 1/2/2
   CVLAN(s)       : 500, 600
   sap-profile    : default-sap-profile
Service Name : Video-Service
SVLAN   : 300
NNI(s)  : 1/1/22, 1/2/3
SAP Id  : 20
   UNIs           : 1/1/1, 1/1/2
   CVLAN(s)       : 10, 20
   sap-profile    : sap-video1
SAP Id  : 30
   UNIs           : 1/1/3
   CVLAN(s)       : 30, 40
   sap-profile    : sap-video2

output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The slot and port number or link aggregate ID for the specified interface.</td>
</tr>
<tr>
<td>Port Type</td>
<td>The type of VLAN Stacking port (UNI or NNI).</td>
</tr>
<tr>
<td>Service Name</td>
<td>The name of the VLAN Stacking service.</td>
</tr>
<tr>
<td>SVLAN</td>
<td>Displays the SVLAN ID associated with the service. Note that SVLAN appears as the field name if the VLAN ID is an SVLAN.</td>
</tr>
<tr>
<td>NNI(s)</td>
<td>VLAN Stacking Network Network Interface ports associated with the service to tunnel SVLAN customer traffic.</td>
</tr>
<tr>
<td>SAP Id</td>
<td>The ID number for the VLAN Stacking Service Access Point that is applied to the service.</td>
</tr>
<tr>
<td>UNIs</td>
<td>VLAN Stacking User Network Interface ports that receive customer traffic.</td>
</tr>
<tr>
<td>CVLAN(s)</td>
<td>Customer VLAN IDs ingressing on UNI ports.</td>
</tr>
<tr>
<td>sap-profile</td>
<td>The name of the SAP profile associated with the SAP.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

- **ethernet-service svlan nni** Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN.
- **ethernet-service sap uni** Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking SAP.
- **show ethernet-service** Displays configuration information for VLAN Stacking Ethernet services.
**MIB Objects**

alaEServiceTable
  alaEServiceID
  alaEServiceSVLAN
alaEServiceNniSvlanTable
  alaEServiceNniSvlanNni
alaEServiceSapTable
  alaEServiceSapID
alaEServiceSapUniTable
  alaEServiceSapUniUni
alaEServiceSapCvlanTable
  alaEServiceSapCvlanCvlan
  alaEServiceSapCvlanMapType
alaEServiceSapProfileTable
  alaEServiceProfileID
**show ethernet-service nni**

Displays configuration information for VLAN Stacking Network Network Interface (NNI) ports.

```
show ethernet-service nni [port chassis/slot/port | linkagg agg_id]
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1).
- **agg_id**: The link aggregate ID number.

**Defaults**

By default, all NNI ports are displayed if a slot/port or link aggregate ID number is not specified.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>slot/port</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>agg_id</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify a slot/port or link aggregate ID number to display information for a single slot/port or link aggregate ID.

**Examples**

```
-> show ethernet-service nni

<table>
<thead>
<tr>
<th>Port</th>
<th>TPID</th>
<th>Legacy BPDU stp</th>
<th>Legacy BPDU mvrp</th>
<th>Transparent Bridging stp</th>
<th>Transparent Bridging mvrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/22</td>
<td>0x8100</td>
<td>Disable</td>
<td>Disable</td>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>1/1/23</td>
<td>0x8100</td>
<td>Disable</td>
<td>Disable</td>
<td>Enable</td>
<td></td>
</tr>
</tbody>
</table>

-> show ethernet-service nni 1/23

<table>
<thead>
<tr>
<th>Port</th>
<th>TPID</th>
<th>Legacy BPDU stp</th>
<th>Legacy BPDU mvrp</th>
<th>Transparent Bridging stp</th>
<th>Transparent Bridging mvrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/23</td>
<td>0x8100</td>
<td>Disable</td>
<td>Disable</td>
<td>Enable</td>
<td></td>
</tr>
</tbody>
</table>
```
output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The slot/port number or link aggregate ID for the NNI port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPID</td>
<td>The vendor TPID value configured for the NNI port.</td>
</tr>
<tr>
<td>stp</td>
<td>Whether Spanning Tree legacy BPDU processing is enabled for the NNI port.</td>
</tr>
<tr>
<td>mvrp</td>
<td>Whether MVRP legacy BPDU processing is enabled for the port.</td>
</tr>
<tr>
<td>Transparent Bridging</td>
<td>Whether transparent bridging is enabled or disabled.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

- **ethernet-service svlan nni**: Configures the switch port as a VLAN Stacking NNI port and associates the port with a customer SVLAN, management SVLAN.
- **ethernet-service nni**: Configures the vendor TPID value and the legacy BPDU processing status for a VLAN Stacking Network Network Interface (NNI).
- **show ethernet-service**: Displays configuration information for VLAN Stacking Ethernet services.

MIB Objects

- `alaEServicePortTable`
  - `alaEServicePortID`
  - `alaEServicePortVendorTpid`
  - `alaEServicePortLegacyStpBpdu`
  - `alaEServicePortLegacyGvrpBpdu`
  - `alaEServicePortTransBridging`
show ethernet-service nni l2pt-statistics

Displays statistics collected for Network Network Interface (NNI) ports.

show ethernet-services nni [port chassis/slot/port | linkagg agg_id] l2pt-statistics

## Syntax Definitions

- **chassis/slot/port**
  
  The chassis, slot, and port number (1/1/6).

- **agg_id**
  
  The link aggregate ID number (0–31).

## Defaults

By default, statistics for all NNI ports is displayed.

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

## Usage Guidelines

- Use the `port chassis/slot/port` or `linkagg agg_id` parameter to display statistics information for a specific switch port or link aggregate ID.

- Make sure the specified port or link aggregate is configured as an NNI port.

## Examples

```
-> show ethernet-service nni l2pt-statistics
Port Rx Mac-Tunnel Mac-tunnel discard
-------------------------------------
1/1/23 1234 2
1/1/24 256 0

-> show ethernet-service nni port 1/1/24 l2pt-statistics
Port Rx Mac-Tunnel Mac-tunnel discard
-------------------------------------
1/1/24 256 0

-> show ethernet-service nni port 1/1/5 l2pt-statistics
ERROR: Port (1/1/5) is not bound to any svlan
```
show ethernet-service nni l2pt-statistics

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The chassis, slot, and port number or link aggregate ID for the NNI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Mac-Tunnel</td>
<td>The total number of frames that were trapped for processing with tunnel MAC.</td>
</tr>
<tr>
<td>Mac-tunnel discard</td>
<td>The total number of discarded frames that were trapped for processing with tunnel MAC.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R2; command was introduced.  
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

clear ethernet-service nni l2pt-statistics  
Clears all NNI port statistics.

show ethernet-service nni  
Displays configuration information for VLAN Stacking NNI ports.

MIB Objects

alaEServiceNNIPortL2ProtocolStatisticsTable
  alaEServiceNNIPortID
  alaEServiceNNIPortL2RxMACTunneledFrames
  alaEServiceNNIPortL2MACtunneledDiscardFrames
clear ethernet-service nni l2pt-statistics

Clears statistics collected for Network Network Interface (NNI) ports.

clear ethernet-services nni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] l2pt-statistics

Syntax Definitions

chassis/slot/port[-port2] The chassis, slot, and port number (1/1/6) on which to clear the statistics. Use a hyphen to specify a range of ports (1/1/6-10).

agg_id[-agg_id2] The link aggregate ID number on which to clear the statistics. Use a hyphen to specify a range of link aggregate IDs (5-10)

Defaults

By default, the statistics for all NNI ports are cleared if a port or link aggregate ID number is not specified.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the port chassis/slot/port[-port2] or linkagg agg_id[-agg_id2] parameter to clear statistics information for specific switch ports or link aggregate IDs.
- Make sure the specified port or link aggregate is configured as an NNI port.

Examples

- clear ethernet-service nni l2pt-statistics
- clear ethernet-service nni port 1/1/6 l2pt-statistics
- clear ethernet-service nni port 1/1/7-10 l2pt-statistics
- clear ethernet-service nni port 1/1/5 l2pt-statistics
  ERROR: Port 1/1/5 is not a network port

- clear ethernet-service nni linkagg 10 l2pt-statistics
- clear ethernet-service nni linkagg 11-15 l2pt-statistics
- clear ethernet-service nni linkagg 20 l2pt-statistics
  ERROR: Port or Linkagg not Vlan Stacking Port

Release History

Release 8.6R2; command was introduced.
Release 8.9R1; Omniswitch 6560 support added.
Related Commands

**show ethernet-service nni l2pt-statistics**  Displays the statistics information collected for NNI ports.

MIB Objects

alaEServiceNNIPortL2GlobalClearStatistics
alaEServiceNNIPortL2ProtocolStatisticsTable
  alaEServiceNNIPortID
  alaEServiceNNIPortL2ClearStats
show ethernet-service uni

Displays a list of UNI ports configured for the switch and the profile association for each port.

show ethernet-service uni [port chassis/slot/port | linkagg agg_id]

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port</td>
<td>The slot and port number (3/1).</td>
</tr>
<tr>
<td>agg_id</td>
<td>The link aggregate ID number.</td>
</tr>
</tbody>
</table>

Defaults

By default, profile information for all UNI ports is displayed if a slot/port or link aggregate ID number is not specified.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify a chassis/slot/port or link aggregate ID number to display information for a single port or link aggregate ID.

Examples

-> show ethernet-service uni

<table>
<thead>
<tr>
<th>Port</th>
<th>UNI Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>uni-profile-default</td>
</tr>
<tr>
<td>1/1/2</td>
<td>multi-site</td>
</tr>
<tr>
<td>1/1/3</td>
<td>multi-site</td>
</tr>
</tbody>
</table>

-> show ethernet-service uni port 1/3

<table>
<thead>
<tr>
<th>Port</th>
<th>UNI Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/3</td>
<td>multi-site</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The chassis/slot/port number or link aggregate ID for the UNI port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNI Profile</td>
<td>The UNI profile associated with the port.</td>
</tr>
</tbody>
</table>
Release History

Release 7.1.1; command introduced.

Related Commands

**ethernet-service sap uni**
Configures the switch port as a VLAN Stacking UNI and associates the port with a VLAN Stacking Service Access Point (SAP).

**ethernet-service uni-profile**
Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.

**ethernet-service uni uni-profile**
Associates a VLAN Stacking UNI profile with a UNI port.

**show ethernet-service uni-profile**
Displays the profile attribute configuration for VLAN Stacking UNI profiles.

MIB Objects

alaEServiceUniProfileTable
- alaEServicePortID
- alaEServicePortProfileID
show ethernet-service uni l2pt-statistics

Displays statistics collected for each tunneling protocol on a per-UNI port basis.

show ethernet-service uni [port chassis/slot/port | linkagg agg_id] l2pt-statistics

Syntax Definitions

chassis/slot/port The chassis, slot, and port number (3/1).
agg_id The link aggregate ID number.

Defaults

By default, statistics information for all UNI ports and associated tunneling protocols is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the port chassis/slot/port or linkagg agg_id parameter to display statistics information for a specific switch port or link aggregate ID.
- Make sure the specified port or link aggregate is configured as a UNI port.
- UNI port statistics are cleared when a switch takeover occurs. However, unless NNI port statistics are cleared, the de-tunnel statistics for a UNI port are not cleared after a takeover. For example, during a takeover, an NNI port that is not on the reloading chassis remains up and the UNI port on the reloading chassis goes down. Even though the UNI port goes down, the de-tunnel statistics for the UNI port are not cleared. However, all other statistics for the UNP port are cleared.

Note. Clearing both UNI and corresponding NNI port statistics after a takeover is highly recommended to ensure old UNI port statistics are not displayed.

Examples

-> show ethernet-service uni L2PT-statistics

<table>
<thead>
<tr>
<th>Port</th>
<th>L2 Protocol</th>
<th>Rx</th>
<th>Peer</th>
<th>Mac Tunnel</th>
<th>De-tunnel</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/5</td>
<td>STP</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>000000:000001</td>
</tr>
<tr>
<td>1/1/5</td>
<td>802.1x</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>10</td>
<td>000000:000001</td>
</tr>
<tr>
<td>1/1/5</td>
<td>802.3ad</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>000000:000001</td>
</tr>
<tr>
<td>1/1/5</td>
<td>802.1ab</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>1/1/5</td>
<td>GVRP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>1/1/5</td>
<td>AMAP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>
VLAN Stacking Commands

show ethernet-service uni l2pt-statistics

1/1/5  OAM  0  0  0  0  -
1/1/5  LACP MARKER  0  0  0  0  -
1/1/5  UDLD  0  0  0  0  -
1/1/5  PAGP  0  0  0  0  -
1/1/5  CDP  0  0  0  0  -
1/1/5  VTP  10  0  10  10  000000:000001
1/1/5  DTP  10  0  10  10  000000:000001
1/1/5  PVST  0  0  0  0  -
1/1/5  VLAN  0  0  0  0  -
1/1/5  UPLINK  0  0  0  0  -
1/1/5  MVRP  0  0  0  0  -

-> show ethernet-service uni port 1/1/4 l2pt-statistics
ERROR: Port (1/4) is not a user port

output definitions

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>UNI port associated with an L2 protocol and L2 protocol statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2 Protocol</td>
<td>The l2 protocol associated with the service UNI port.</td>
</tr>
<tr>
<td>Rx</td>
<td>The total number of frames received by the protocol on the port that are trapped for processing.</td>
</tr>
<tr>
<td>Peer</td>
<td>The total number of tunneled frames received by the protocol on the port that are trapped for processing and peered.</td>
</tr>
<tr>
<td>Mac Tunnel</td>
<td>The total number of tunneled frames received by the protocol on the port that are trapped for processing and MAC tunneled.</td>
</tr>
<tr>
<td>Mac De-tunnel</td>
<td>The total number of tunneled frames received by the protocol on the port that are trapped for processing and MAC de-tunneled.</td>
</tr>
<tr>
<td>Source MAC</td>
<td>Specifies the source MAC address of the last frame of the protocol on the port trapped in CPU.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R2; command was introduced.
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

clear ethernet-service uni l2pt-statistics  Clears the tunneling protocol statistics on UNI ports.
show ethernet-service uni                  Displays a list of UNI ports configured for the switch and the profile association for each port.

MIB Objects

alaEServiceUNIPortL2ProtocolStatisticsTable
  alaEServiceUNIPortID
  alaEServiceUNIPortL2ProtocolID
  alaEServiceUNIPortL2RxFrames
  alaEServiceUNIPortL2PeeredFrames
  alaEServiceUNIPortL2MACTunneledFrames
  alaEServiceUNIPortL2MACDeTunneledFrames
  alaEServiceUNIPortL2LastSourceMAC
clear ethernet-service uni l2pt-statistics

Clears tunneling protocol statistics collected for UNI ports.

```
clear ethernet-service uni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] l2pt-statistics
```

**Syntax Definitions**

- `chassis/slot/port[-port2]` : The chassis, slot, and port number (1/1/6) on which to clear the statistics. Use a hyphen to specify a range of ports (1/1/6-10).
- `agg_id[-agg_id2]` : The link aggregate ID number on which to clear the statistics. Use a hyphen to specify a range of link aggregate IDs (5-10)

**Defaults**

By default, tunneling protocol statistics are cleared on all UNI ports if a port or link aggregate ID number is not specified.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `port chassis/slot/port[-port2]` or `linkagg agg_id[-agg_id2]` parameter to clear statistics information for specific switch ports or link aggregate IDs.
- Make sure the specified port or link aggregate is configured as a UNI port.
- UNI port statistics are cleared when a switch takeover occurs. However, unless NNI port statistics are cleared, the de-tunnel statistics for a UNI port are not cleared after a takeover. For example, during a takeover, an NNI port that is not on the reloading chassis remains up and the UNI port on the reloading chassis goes down. Even though the UNI port goes down, the de-tunnel statistics for the UNI port are not cleared. However, all other statistics for the UNP port are cleared.

**Note.** Clearing both UNI and corresponding NNI port statistics after a takeover is highly recommended to ensure old UNI port statistics are not displayed.

**Examples**

```
-> clear ethernet-service uni l2pt-statistics

-> clear ethernet-service uni port 1/1/1 l2pt-statistics
-> clear ethernet-service uni port 1/1/7-10 l2pt-statistics
-> clear ethernet-service uni port 1/1/6 l2pt-statistics
ERROR: Port 1/1/6 is not a user port
```
VLAN Stacking Commands

-> clear ethernet-service uni linkagg 10 l2pt-statistics
-> clear ethernet-service uni linkagg 11-15 l2pt-statistics
-> clear ethernet-service uni linkagg 20 l2pt-statistics
ERROR: Port or Linkagg not Vlan Stacking Port

Release History

Release 8.6R2; command was introduced.
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

show ethernet-service uni l2pt-statistics
  Displays tunneling protocol statistics on a per-UNI port.

MIB Objects

alaEServiceUNIPortL2GlobalClearStatistics
alaEServiceUNIPortL2ProtocolStatisticsClearTable
  alaEServiceUNIPortClearID,
  alaEServiceUNIPortL2ClearStats
show ethernet-service uni-profile

Displays the profile attribute configuration for VLAN Stacking User Network Interface (UNI) profiles.

**show ethernet-service uni-profile [uni_profile_name]**

### Syntax Definitions

**uni_profile_name**

An alphanumeric string. Use quotes around the string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

### Defaults

By default, all UNI profiles are displayed if a UNI profile name is not specified with this command.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Specify a UNI profile name to display attributes for a single UNI profile.
- UNI profile information is displayed based on the switch platform. For example, UNI profile settings to process CISCO control packets and custom L2 protocol assignments for UNI profiles are supported only on the OmniSwitch 6465, OmniSwitch 6860, OmniSwitch 6860N, and OmniSwitch 6865, so that information is displayed only on those switches.

### Examples

Sample output on an OmniSwitch 6465, OmniSwitch 6860, OmniSwitch 6860N, and OmniSwitch 6865:

```
-> show ethernet-service uni-profile
Profile Name: default-uni-profile
  Tunnel MAC : 01:00:0c:cd:cd:d0,
  STP : tunnel, 802.1x : drop, 802.3ad : peer, 802.1ab : drop,
  MVRP: tunnel, AMAP : drop, OAM : peer, LACPMARKER : peer,
  UDLD: peer, PAGP : drop, CDP : drop, VTP : drop,
  DTP : drop, PVST : drop, VLAN : drop, UPLINK : drop,
  802.1AB Tagged : drop, 802.1AB UnTagged: drop, 802.1AB Mode : default
Profile Name: ieee-drop-all
  All IEEE Mac Addresses : 01:80:C2:00:00:00 - 01:80:C2:00:00:FF : drop
Profile Name: ieee-fwd-all
  All IEEE Mac Addresses : 01:80:C2:00:00:00 - 01:80:C2:00:00:FF : tunnel,
  Pause Frame : 01:80:C2:00:00:01 : drop,
  Mac specific control frame : 01:80:C2:00:00:04 : drop
```
Profile Name: uni-prof1
  Tunnel MAC : 01:00:0c:cd:cd:d0,
  STP : tunnel,  802.1x : drop,  802.3ad : peer,  802.1ab : drop,
  MVRP: tunnel,  AMAP : drop,  OAM : peer,  LACPMARKER : peer,
  UDLD: peer,  CDP : drop,  VLAN : drop,  UPILINK : drop,
  802.1AB Tagged : drop,  802.1AB UnTagged: drop,  802.1AB Mode : default

output definitions

Profile Name
The name of the UNI profile.

Tunnel MAC
The MAC address used for MAC tunneling.

PROTOCOL: action
The protocol and configured action:
- peer—The UNI port is participating in the specified protocol.
- drop—Discards the specified PDU.
- tunnel—The PDU is tunneled across the provider network without
  modifying the MAC address.
- mac-tunnel—The PDU is tunneled across the provider network after
  changing the destination MAC address to the tunnel MAC address.

Custom L2 Protocol
The name of a custom L2 protocol that is assigned to the UNI profile.

Sample output on an OmniSwitch 6900:
-> show ethernet-service uni-profile

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Stp</th>
<th>802.1x</th>
<th>802.3ad</th>
<th>MVRP</th>
<th>AMAP</th>
<th>Both</th>
<th>Tagged</th>
<th>Untagged</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-uni-profile</td>
<td>tunnel</td>
<td>drop</td>
<td>peer</td>
<td>tunnel</td>
<td>drop</td>
<td>drop</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>lldp-tag-untag</td>
<td>tunnel</td>
<td>drop</td>
<td>peer</td>
<td>tunnel</td>
<td>drop</td>
<td>-</td>
<td>tunnel</td>
<td>drop</td>
</tr>
<tr>
<td>uprofile-video1</td>
<td>tunnel</td>
<td>drop</td>
<td>peer</td>
<td>drop</td>
<td>tunnel</td>
<td>drop</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

output definitions

Profile Name
The name of the UNI profile.

PROTOCOL: action
The protocol and configured action:
- peer—The UNI port is participating in the specified protocol.
- drop—Discards the specified PDU.
- tunnel—The PDU is tunneled across the provider network without
  modifying the MAC address.

Release History
Release 7.1.1; command introduced.
Release 8.6R1; “Tunnel MAC” field added, additional protocol fields added to display action for CISCO
PDUs, custom L2 protocol entry names and action included in display output.
Release 8.6R2; “802.1AB Both”, “802.1AB Tagged”, “802.1AB Untagged”, and “802.1AB Mode” fields added.
**Related Commands**

- `ethernet-service uni-profile` Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.
- `ethernet-service uni-profile inbound 802.1ab` Configures the treatment of Layer 2 tagged and untagged 802.1AB control frames that are received on UNI ports.
- `ethernet-service uni uni-profile` Associates a VLAN Stacking UNI profile with a UNI port.
- `ethernet-service custom-L2-protocol` Creates a custom L2 protocol MAC address entry with an optional mask, EtherType, or SSAP/DSAP protocol identifier.
- `ethernet-service uni-profile custom-L2-protocol` Assigns a custom L2 protocol MAC address entry to a UNI profile.
- `show ethernet-service uni` Displays the profile associations for VLAN Stacking UNI ports.

**MIB Objects**

alaEServiceUNIProfileTable
  - alaEServiceUNIProfileID
  - alaEServiceUNIProfileStpBpduTreatment
  - alaEServiceUNIProfile8021xTreatment
  - alaEServiceUNIProfile8021ABTreatment
  - alaEServiceUNIProfile8023adTreatment
  - alaEServiceUNIProfileMvrpTreatment
  - alaEServiceUNIProfileAmapTreatment
  - alaEServiceUNIProfileVtpTreatment
  - alaEServiceUNIProfileVlanTreatment
  - alaEServiceUNIProfileUplinkTreatment
  - alaEServiceUNIProfileUdldTreatment
  - alaEServiceUNIProfilePvstTreatment
  - alaEServiceUNIProfilePagpTreatment
  - alaEServiceUNIProfileLacpmarkerTreatment
  - alaEServiceUNIProfileDtpTreatment
  - alaEServiceUNIProfileCdpTreatment
  - alaEServiceUNIProfileTunnelMac
  - alaEServiceUNIProfileIeeeMacTreatment
  - alaEServiceUNIProfileOamTreatment
  - alaEServiceUNIProfile8021ABTagTreatment
  - alaEServiceUNIProfile8021ABUnTagTreatment

alaEServiceUNIProfileL2CustomProtocolTable
  - alaEServiceUNIProfileL2CustomID
  - alaEServiceUNIProfileL2CustomProtocolID
  - alaEServiceUNIProfileL2CustomProtocolType
show ethernet-service custom-l2-protocol

Displays the custom L2 protocol configuration for the switch.

show ethernet-service custom-l2-profile [custom_protocol_name]

Syntax Definitions

custom_protocol_name                   The name of a configured custom L2 protocol entry.

Defaults

By default, all custom L2 protocol entries are displayed if a custom L2 protocol name is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

• Specify a custom L2 protocol name to display attributes for a specific custom protocol entry.

• A custom L2 protocol entry is assigned to a UNI profile. Use the show ethernet-service uni-profile command to display the custom L2 protocol entries assigned to a UNI profile.

Examples

-> show ethernet-service custom-l2-protocol
Custom L2 Protocol    Mac    Mask    Ether-Type   Sub-Type
                        (or)   (or)   (or)       (or)
                        Ssap/Dsap    Pid
--------------------------------------------------------------------------
tunnel-mac-ethersubtype 01:80:c2:00:11:11   -   0x5556       120
                        0x5556       -
tunnel-mac-ethertype     01:80:c2:00:11:11   -   0x5555       -
tunnel-mac-ssap/dsap     01:80:c2:00:11:11   -   0x43/0x43      3
                        0x43/0x43      -
tunnel-mac              01:80:c2:00:11:11   -   -            -
tunnel-mac-range        01:80:c2:00:11:11 ff:ff:ff:ff:ff:00   -   -
discard-mac-range       01:80:c2:00:11:11 ff:ff:ff:00:ff:ff   -   -
--------------------------------------------------------------------------

-> show ethernet-service custom-l2-protocol tunnel-mac-range
Custom L2 Protocol    Mac    Mask    Ether-Type   Sub-Type
                        (or)   (or)   (or)       (or)
                        Ssap/Dsap    Pid
--------------------------------------------------------------------------
tunnel-mac-range       01:80:c2:00:11:11 ff:ff:ff:ff:ff:00   -   -
--------------------------------------------------------------------------
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom L2 Protocol</td>
<td>The name of the custom L2 protocol entry.</td>
</tr>
<tr>
<td>Mac</td>
<td>The multicast MAC address for the custom L2 protocol entry.</td>
</tr>
<tr>
<td>Mask</td>
<td>The MAC address mask to specify a range of MAC addresses.</td>
</tr>
<tr>
<td>Ether-Type (or) Ssap/Dsap</td>
<td>The EtherType or SSAP/DSAP value for the MAC address entry.</td>
</tr>
<tr>
<td>Sub-Type (or) Pid</td>
<td>The optional Sub-Type value or the PID value for the MAC address entry.</td>
</tr>
<tr>
<td></td>
<td>• A Sub-Type value is optionally entered when an EtherType value is specified.</td>
</tr>
<tr>
<td></td>
<td>• A PID value is specified when an SSAP/DSAP value is specified.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R1; command introduced.
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

- `ethernet-service custom-L2-protocol` Creates a custom L2 protocol MAC address entry with an optional mask, EtherType, or SSAP/DSAP protocol identifier.
- `ethernet-service uni-profile custom-L2-protocol` Assigns a custom L2 protocol entry to a UNI profile.
- `show ethernet-service uni-profile` Displays the UNI profile configuration for the switch, which includes any custom L2 protocol assignments.

MIB Objects

- `alaEServiceCustomL2ProtocolTable`
- `alaEServiceCustomL2ProtocolName`
- `alaEServiceCustomL2ProtocolMac`
- `alaEServiceCustomL2ProtocolMask`
- `alaEServiceCustomL2ProtocolEtherType`
- `alaEServiceCustomL2ProtocolEtherSubType`
- `alaEServiceCustomL2ProtocolSsap`
- `alaEServiceCustomL2ProtocolDsap`
- `alaEServiceCustomL2ProtocolPid`
- `alaEServiceCustomL2ProtocolRowStatus`
show ethernet-service uni-profile l2pt-statistics

Displays the profile statistics collected for User Network Interface (UNI) profiles. Statistics are collected for all protocol frames (including custom L2 protocols) that are received on all ports that are bound to the UNI profile.

show ethernet-service uni-profile [uni_profile_name] l2pt-statistics

Syntax Definitions

uni_profile_name The name of the UNI profile.

Defaults

By default, statistics for all UNI profiles are displayed if a UNI profile name is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify a UNI profile name to display the statistics for a single UNI profile.

Examples

-> show ethernet-service uni-profile Profile-1 l2pt-statistics
UNI Profile: Profile-1
Total RX: 0,
L2 Protocol:
  STP
    Rx: 0,
    Hardware processing: FWD,
  GVRP, MVRP
    Rx: 0,
    Hardware processing: FWD,
  802.1ab
    Rx: 0,
    Hardware processing: DROP,
  AMAP
    Rx: 0,
    Hardware processing: DROP,
  802.3ad, OAM, LACPMARKER
    Rx: 0,
    Hardware processing: CPU,
Rx:                                      0,
Hardware processing:                    DROP,
PAGP, UDLD, CDP, DTP, VTP, PVST, VLAN, UPLINK
Rx:                                      0,
Hardware processing:                    CPU,
802.1ab Tagged                            
Rx:                                      0,
Hardware processing:                    DROP,
802.1ab Untagged                          
Rx:                                      0,
Hardware processing:                    DROP,

output definitions

<table>
<thead>
<tr>
<th>UNI Profile</th>
<th>The UNI profile associated with the port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total RX</td>
<td>The total number of protocol frames received on the port that is associated with the UNI profile.</td>
</tr>
<tr>
<td>L2 Protocol</td>
<td>The protocol for which the statistics are collected.</td>
</tr>
<tr>
<td>Rx</td>
<td>The number of frames received for the specific protocol.</td>
</tr>
<tr>
<td>Hardware processing</td>
<td>Displays the configured hardware action.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R2; command was introduced.

Related Commands

clear ethernet-service uni-profile l2pt-statistics
Clears the statistics for all UNI profiles.

ethernet-service uni-profile
Creates a UNI profile that is used to specify how to process control packets ingressing on UNI ports.

ethernet-service uni uni-profile
Associates a VLAN Stacking UNI profile with a UNI port.

show ethernet-service uni
Displays the profile associations for VLAN Stacking UNI ports.

show ethernet-service uni l2pt-statistics
Displays tunneling protocol statistics for UNI ports.

MIB Objects

alaEServiceUNIProfileL2ProtocolTotalStatisticsTable
alaEServiceUNIProfile
alaEServiceUNIProfileL2ProtocolTotalRxFrames
alaEServiceUNIProfileL2ProtocolStatisticsTable
alaEServiceUNIProfileID
alaEServiceUNIProfileL2ProtocolIndex
alaEServiceUNIProfileL2ProtocolRxFrames
alaEServiceUNIProfileL2ProtocolTreatment
alaEServiceUNIProfileCustomL2ProtocolStatisticsTable
alaEServiceUNIProfileCustomL2StatsProfileID
alaEServiceUNIProfileCustomL2ProtocolIndex
alaEServiceUNIProfileCustomL2ProtocolRxFrames
VLAN Stacking Commands

show ethernet-service uni-profile l2pt-statistics

alaEServiceUNIProfileCustomL2ProtocolTreatment
clear ethernet-service uni-profile l2pt-statistics

Cleans the protocol statistics collected for UNI profiles.

clear ethernet-service uni-profile [uni_profile_name] l2pt-statistics

Syntax Definitions

uni_profile_name The name of the UNI profile.

Defaults

By default, statistics are cleared for all UNI profiles.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify a UNI profile name to clear the statistics for a single UNI profile.

Examples

-> clear ethernet-service uni-profile uni-profile 1 l2pt-statistics

Release History

Release 8.6R2; command was introduced.

Related Commands

show ethernet-service uni-profile l2pt-statistics Displays the statistics of all protocols configured per UNI port.

MIB Objects

alaEServiceUNIProfileL2GlobalClearStatistics
alaEServiceUNIProfileL2ProtocolTotalStatisticsTable
alaEServiceUNIProfile
alaEServiceUNIProfileL2ProtocolClearStats
show ethernet-service mac-tunneling

Displays the global MAC tunneling status for the switch.

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
Any changes to the global MAC tunneling status requires a switch reload to activate.

Examples

-> show ethernet-service mac-tunneling
Mac-Tunneling Feature: enable

-> ethernet-service mac-tunneling disable
INFO :Changed mac-tunnel feature status will take effect if command is saved on next switch reboot

-> show ethernet-service mac-tunneling
(*=new mac-tunneling feature will be applied after reboot)
Mac-Tunneling Feature: disable*

Release History
Release 8.6R1; command introduced.
Release 8.9R1; Omniswitch 6560 support added.

Related Commands

ethernet-service mac-tunneling Configures the global MAC tunneling status for the switch

MIB Objects
alaEServiceGlobals
  alaEServiceGlobalMacTunneling
show ethernet-service sap-profile

Displays the profile attribute configuration for VLAN Stacking Service Access Point (SAP) profiles.

show ethernet-service sap-profile sap_profile_name

Syntax Definitions

uni-profile-name An alphanumeric string. Use quotes around the string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

Defaults

By default, all SAP profiles are displayed if a SAP profile name is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specify a SAP profile name to display attributes for a single SAP profile.
- The ingress bandwidth value is displayed in megabytes.

Examples

-> show ethernet-service sap-profile

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Ingr/Egr Bw</th>
<th>Ingr Bw Sharing</th>
<th>Inner Tag</th>
<th>Priority Option</th>
<th>Priority Mapping</th>
<th>Priority Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-sap-profile</td>
<td>0/0</td>
<td>Enable</td>
<td>Preserve</td>
<td>fixed</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>map_pbit</td>
<td>0/0</td>
<td>Enable</td>
<td>Preserve</td>
<td>in-out</td>
<td>P</td>
<td></td>
</tr>
<tr>
<td>sap1</td>
<td>24324/0</td>
<td>NA</td>
<td>Preserve</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>sap_1</td>
<td>0/0</td>
<td>NA</td>
<td>Preserve</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

-> show ethernet-service sap-profile sap-video1

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Ingr/Egr Bw</th>
<th>Ingr Bw Sharing</th>
<th>Inner Tag</th>
<th>Priority Option</th>
<th>Priority Mapping</th>
<th>Priority Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap-video1</td>
<td>20</td>
<td>Disable</td>
<td>Preserve</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 7-77
output definitions

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>The name of the SAP profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingr/Egr Bw</td>
<td><strong>Ingress Egress Bandwidth</strong> - The maximum amount of ingress and egress bandwidth to allow for SAP ports.</td>
</tr>
<tr>
<td>Ingr Bw Sharing</td>
<td><strong>Ingress Bandwidth Sharing</strong> - The status of bandwidth sharing (enable, disable, or NA). If enabled, the ingress bandwidth value is shared across all SAP ports and CVLANs. If disabled, the bandwidth value is not shared and applied to individual SAP ports and CVLANs.</td>
</tr>
<tr>
<td>Inner Tag Option</td>
<td>Indicates how the CVLAN tag is processed (translate or preserve). If set to preserve, the CVLAN tag is retained and the SVLAN is added to the frame. If set to translate, the CVLAN tag is changed to the SVLAN tag.</td>
</tr>
<tr>
<td>Priority Mapping</td>
<td>Indicates how the priority value is configured for the SVLAN (NA, in-out or fixed). If set to in-out, the CVLAN priority value is mapped to the SVLAN. If set to fixed, a user-specified priority value is used for the SVLAN priority.</td>
</tr>
<tr>
<td>Priority Value</td>
<td>Indicates the priority value mapped to the SVLAN (NA, default 0, a number, P, or DSCP). A number indicates a fixed, user-specified value is used; P indicates the CVLAN 802.1p bit value is used; DSCP indicates the CVLAN DSCP value is used.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

- **ethernet-service sap-profile** Creates a profile for a VLAN Stacking Service Access Point (SAP).
- **ethernet-service sap** Creates a VLAN Stacking SAP and associates the SAP with a service and SAP profile.
- **ethernet-service sap-profile** Specifies a different SAP profile for the SAP.
- **show ethernet-service sap** Displays configuration information for VLAN Stacking SAPs.

MIB Objects

- alaEServiceSapProfileTable
  - alaEServiceSapProfileID
  - alaEServiceSapProfileCVLANTreatment
  - alaEServiceSapProfilePriorityMapMode
  - alaEServiceSapProfileFixedPriority
  - alaEServiceSapProfileIngressBW
  - alaEServiceSapProfileEgressBW
  - alaEServiceSapProfileBandwidthShare
**loopback-test**

Configures a wire-rate hardware loopback test profile and enables or disables the activation of the profile. The loopback test profile specifies the switch attributes that are required to conduct an ingress or egress loopback operation on a switch port.

```
loopback-test profile_name destination-mac dest_address {port chassis/slot/port | linkagg agg_id}
source-mac src_address vlan vlan_id [type {inward | outward {sap sap_id}}]
```

```
loopback-test profile_name admin-state {enable | disable}
```

[no] loopback-test profile_name

---

**Syntax Definitions**

- **profile_name**: Alphanumeric string of up to 31 characters. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).
- **src_address**: A unique source MAC address for the test frame.
- **dest_address**: A unique destination MAC address for the test frame.
- **vlan_id**: The VLAN ID of the test frame. Always use the outer VLAN ID.
- **chassis/slot/port**: The switch port number to use for the loopback test.
- **agg_id**: The linkagg ID for the loopback test. *This is currently not supported.*
- **inward**: Sets the type of loopback test to ingress.
- **outward**: Sets the type of loopback test to egress.
- **sap_id**: An existing Service Access Point (SAP) ID to use for an outward loopback test. *This parameter is supported on the OmniSwitch 6465.* See “Usage Guidelines - OmniSwitch 6465” on page 7-80.
- **enable**: Enables the loopback test profile.
- **disable**: Disables the loopback test profile.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>inward</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- Use the `no` form of this command to delete a loopback profile.

- Use the `loopback-test admin-state enable` command to enable the loopback test profile on the specified port. When the profile is enabled, the loopback operation is enabled for the port.

- Use the `loopback-test admin-state disable` command to disable the loopback operation for the specified port.

- The `loopback-test admin-state enable` command does not appear in the `show configuration snapshot` command display; it is not saved to the switch configuration file.

- When a port is configured as outward loopback port, it goes “out-of-service” and will no longer carry customer traffic but remains active for test frame traffic. However, an inward loopback port remains “in-service” and will continue to carry customer traffic as well as test frame traffic.

- Only Layer 2 loopback tests are supported, so test frames are not routed. As a result, the loopback test operation will only swap the source and destination MAC address of bridged test frames.

- L3 frames should be used for test frames and L3 headers should be included in test frames. Loopback will not be possible with pure L2 frames.

- Traffic with all the valid CVLANs, which are part of the SVLAN gets looped-back, as hardware loopback cannot identify which CVLAN traffic to loopback.

- During outward loopback test, port will enter MAC-loopback, STP and Source Learning will be disabled on that port.

- In outward UNI/NNI loopback, destination MAC is learned as static MAC on loopback port on `loopback-test enable` and is removed on `loopback-test disable`. This destination MAC is not displayed in `show mac-learning` command.

- The destination MAC address for the test frame must be unique to the network and must not be used anywhere in the device.

- The destination MAC address, source MAC address, loopback-port and VLAN ID are the mandatory parameters for configuring the hardware loopback profile.

**Usage Guidelines - OmniSwitch 6465**

Consider the following differences when configuring a loopback test profile on an OmniSwitch 6465:

- The `loopback-test admin-state enable` command is saved to the switch configuration file. This allows a test to automatically start after the switch reboots.

- A maximum of 28 inward and 8 outward loopback profiles can be configured, but only 2 profiles can be enabled at any given time.

- When defining an inward loopback test profile, specifying a source MAC address and VLAN ID is optional.

- When defining an outward loopback test profile, specifying a source MAC address or SAP ID is optional.

- A SAP ID can be specified for outward loopback test profiles; not supported with inward loopback test profiles. If a SAP ID is not specified, then the SAP with the lowest ID number is used by default.

- If the loopback port is administratively down, then an outward loopback test cannot be started.
The test frame does not have to be an L3 frame; both L2 and L3 test frames are supported.

The hardware loopback feature and CPE Test Head feature can both be operational at the same time. However, Test-OAM and hardware loopback cannot be configured on the same port.

**Usage Guidelines - OmniSwitch 6560 and 6570M**

Consider the following differences when configuring a loopback test profile on an OmniSwitch 6560 or OmniSwitch 6570M:

- The `loopback-test admin-state enable` command is saved to the switch configuration file. This allows a test to automatically start after the switch reboots.
- A maximum of 28 inward and 8 outward loopback profiles can be configured and all the 36 profiles can be enabled at any given time.
- When defining an outward loopback test profile, specifying a VLAN ID is optional and SAP ID is not required.
- When defining an inward loopback test profile, specifying a source MAC address and type is optional.

**Examples**

The following example creates an ingress loopback test profile:

```
-> loopback-test PE1-inward-UNI destination-mac 00:00:00:cc:aa:bb port 1/1/2
    source-mac 00:00:00:dd:aa:01 vlan 1001 type inward
```

The following examples create egress loopback test profiles (the “PE3-outward-UNI” profile specifies a SAP ID, which is supported on the OmniSwitch 6465 and OmniSwitch 6560):

```
-> loopback-test PE2-outward-UNI destination-mac 00:00:00:cc:ab:bb port 1/1/2
    source-mac 00:00:00:dd:ab:01 vlan 1001 type outward
```

The following command examples enable and disable a loopback test profile:

```
-> loopback-test inward1 admin-state enable
-> loopback-test outward1 admin-state disable
-> loopback-test outward1 admin-state enable
```

**Release History**

Release 8.6R1; command was introduced.
Release 8.7R1; `sap` parameter added.
Release 8.9R1; Hardware loopback-test support added for OmniSwitch 6560.
Release 8.9R2; Hardware loopback-test support added for OmniSwitch 6570M.

**Related Commands**

- `show loopback-test` Displays the profile configuration for a loopback test profile.

**MIB Objects**

- `alaTestHwLoopbackProfileTable`
- `alaTestHwLoopbackProfileName`
- `alaTestHwLoopbackSourceMac`
- `alaTestHwLoopbackDestinationMac`
- `alaTestHwLoopbackVlan`
alaTestHwLoopbackPort
alaTestHwLoopbackType
alaTestHwLoopbackSapId
alaTestHwLoopbackPortPktCounter
alaTestHwLoopbackPortByteCounter
alaTestHwLoopbackProfileStatus
alaTestHwLoopbackProfileRowStatus
show loopback-test

Displays the profile configuration for a hardware loopback test profile.

show loopback-test [profile_name] [counters]

Syntax Definitions

profile_name The name of an existing hardware loopback test profile.
counters Counters for given or all loopback test profiles.

Defaults

By default, all profiles are displayed if a profile name is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the profile_name parameter to display the loopback test configuration for a specific profile.
- This command will display “Any” in the “Src-Mac”, “Vlan”, or “SapId” fields if the following optional parameters are not specified when configuring a loopback test on an OmniSwitch 6560, OmniSwitch 6570M and OmniSwitch 6465:
  - Optional inward loopback test parameters: source MAC address and VLAN ID.
  - Optional outward loopback test parameters: source MAC address and SAP ID.
- Hardware counters are displayed only when the test profile is enabled.

Examples

```
-> show loopback-test
Profile-Name  Src-Mac          Dest-Mac          Vlan    Port    Type    Status  SapId
------------+-----------------+-----------------+------+--------+--------+-------+-----+
prof1-out    00:00:00:00:00:05 00:00:00:00:00:04  1000   1/1/11  Outward   Enable
prof2-out    00:00:00:00:00:05 00:00:00:00:00:05  2000   1/1/12  Outward  Disable
prof4-out    00:11:11:11:11:11 00:22:22:22:22:22   199      1/1/7  Outward    Config  1
prof5-in     Any               00:da:95:22:33:10  Any     1/1/8   Inward   Enable
prof6-in     Any               00:da:95:22:33:09  Any     1/1/2   Inward   Config
prof7-out    Any               00:da:95:22:33:07  5       1/1/1   Outward Config  10
prof8-in     Any               00:da:95:22:33:06  Any     1/1/10  Inward Config
Total Entries = 9
```
show loopback-test

Profile-Name | Port     | Type      | Status | Packet Counters | Byte Counters
--------------|----------|-----------|--------|----------------|----------------
prof1-out     | 1/1/11   | Outward   | Enable | 1267025494     | 633512760908   
prof5-in      | 1/1/8    | Inward    | Enable | 217995         | 76000000      

Profile-Name | Port     | Type      | Status | Packet Counters | Byte Counters
--------------|----------|-----------|--------|----------------|----------------
prof1-out     | 1/1/11   | Outward   | Enable | 1267025494     | 633512760908   
prof5-in      | 1/1/8    | Inward    | Enable | 217995         | 76000000      

Profile-Name | Port     | Type      | Status | Packet Counters | Byte Counters
--------------|----------|-----------|--------|----------------|----------------
prof1-out     | 1/1/11   | Outward   | Enable | 1267025494     | 633512760908   
prof5-in      | 1/1/8    | Inward    | Enable | 217995         | 76000000      

Profile-Name | Port     | Type      | Status | Packet Counters | Byte Counters
--------------|----------|-----------|--------|----------------|----------------
prof1-out     | 1/1/11   | Outward   | Enable | 1267025494     | 633512760908   
prof5-in      | 1/1/8    | Inward    | Enable | 217995         | 76000000      

Profile-Name | Port     | Type      | Status | Packet Counters | Byte Counters
--------------|----------|-----------|--------|----------------|----------------
prof1-out     | 1/1/11   | Outward   | Enable | 1267025494     | 633512760908   
prof5-in      | 1/1/8    | Inward    | Enable | 217995         | 76000000      

Profile-Name | Port     | Type      | Status | Packet Counters | Byte Counters
--------------|----------|-----------|--------|----------------|----------------
prof1-out     | 1/1/11   | Outward   | Enable | 1267025494     | 633512760908   
prof5-in      | 1/1/8    | Inward    | Enable | 217995         | 76000000      

Release History

Release 8.6R1; command was introduced.
Release 8.7R1: “SapId” field added.

Related Commands

loopback-test Configures a wire-speed Ethernet loopback test profile and enables or disables the activation of the profile.

MIB Objects

N/A
clear loopback-test counters

Clears the hardware counters of all the loopback test profiles.

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples

-> clear loopback-test counters

Release History
Release 8.6R1; command was introduced.

Related Commands

loopback-test

Configures a wire-speed Ethernet loopback test profile and enables or disables the activation of the profile.

MIB Objects
N/A
The Spanning Tree Algorithm and Protocol (STP) is a self-configuring algorithm that maintains a loop-free topology while providing data path redundancy and network scalability. Based on the IEEE 802.1D standard, the OmniSwitch STP implementation distributes the Spanning Tree load between the primary management module and the network interface modules. This functionality improves network robustness by providing a Spanning Tree that continues to respond to BPDUs and port link up and down states in the event of a fail over to a backup management module or switch.

In addition to a distributed architecture, this implementation also provides the following Spanning Tree features:

- Automatic configuration of a physical topology into a single Spanning Tree to ensure that there is only one data path between any two switches.
- Fault tolerance within the network topology. The Spanning Tree is reconfigured in the event of a data path or bridge failure or when a new switch is added to the topology.
- Support for four Spanning Tree protocols: 802.1D (STP), 802.1W (RSTP), and 802.1Q 2005 (MSTP).
- A flat Spanning Tree operating mode. If STP or RSTP is used, this mode applies a single STP instance across all VLANs. If MSTP is used, this mode applies a single STP instance to each Multiple Spanning Tree Instance (MSTI), which identifies a set of VLANs.
- A per-VLAN Spanning Tree operating mode that applies a single STP instance for each defined VLAN on the switch.
- An STP topology that includes 802.1Q tagged ports and link aggregate logical ports in the calculation of the physical topology.

MIB information for Distributed Spanning Tree commands is as follows:

*Filename:* ALCATEL-IND1-VLAN-STP-MIB.mib  
*Module:* alcatelIND1VLANSTPMIB
A summary of the available commands is listed here:

| Bridge commands          | spantree mode  
|                         | spantree protocol  
|                         | spantree priority  
|                         | spantree hello-time  
|                         | spantree max-age  
|                         | spantree forward-delay  
|                         | spantree bpdu-switching  
|                         | spantree path-cost-mode  
|                         | spantree vlan admin-state  
|                         | spantree auto-vlan-containment  
|                         | show spantree  
|                         | show spantree cist  
|                         | show spantree msti  
|                         | show spantree vlan  
|                         | show spantree mode  
| Port commands           | spantree cist  
|                         | spantree vlan  
|                         | spantree priority  
|                         | spantree cist path-cost  
|                         | spantree msti path-cost  
|                         | spantree vlan path-cost  
|                         | spantree cist mode  
|                         | spantree loop-guard  
|                         | spantree vlan mode  
|                         | spantree cist connection  
|                         | spantree vlan connection  
|                         | spantree cist admin-edge  
|                         | spantree vlan admin-edge  
|                         | spantree cist auto-edge  
|                         | spantree vlan auto-edge  
|                         | spantree cist restricted-role  
|                         | spantree vlan restricted-role  
|                         | spantree cist restricted-tcn  
|                         | spantree vlan restricted-tcn  
|                         | spantree cist txholdcount  
|                         | spantree vlan txholdcount  
|                         | show spantree ports  
|                         | show spantree cist ports  
|                         | show spantree msti ports  
|                         | show spantree vlan ports  
| MST region commands     | spantree mst region name  
|                         | spantree mst region revision-level  
|                         | spantree mst region max-hops  
|                         | show spantree mst  
| MST instance commands   | spantree msti  
|                         | spantree msti vlan  
|                         | show spantree msti vlan-map  
|                         | show spantree cist vlan-map  
|                         | show spantree map-msti  
| PVST+ commands          | spantree pvst+compatibility  
|                         |  

**spantree mode**

Selects the flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch. These modes are exclusive; however, it is not necessary to reboot the switch when the STP modes are changed.

**spantree mode {flat | per-vlan}**

---

**Syntax Definitions**

- **flat**
  One Spanning Tree instance per switch.
- **per-vlan**
  One Spanning Tree instance for each VLAN configured on a switch.

---

**Defaults**

By default, the Spanning Tree mode for the switch is set to per-VLAN.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The Multiple Spanning Tree Protocol (MSTP), as defined in the IEEE 802.1Q 2005 standard, is only supported on switches operating in the flat Spanning Tree mode.

- If standard STP or RSTP is used when the switch is running in the flat mode, a single STP instance is applied across all VLANs. For example, if a port belonging to VLAN 10 and a port belonging to VLAN 20 connect to the same switch together, then STP blocks one of these ports.

- If MSTP is used when the switch is running in the flat mode, a single STP instance is applied to each Multiple Spanning Tree Instance (MSTI). Each MSTI represents a set of VLANs.

- Flat Spanning Tree mode supports fixed (untagged) and 802.1Q tagged ports in each VLAN. However, Bridge Protocol Data Units (BPDUs) are always untagged.

- If the per-VLAN mode is selected, a single Spanning Tree instance is enabled for each VLAN configured on the switch. For example, if there are five VLANs configured on the switch, then there are five separate Spanning Tree instances. In essence, a VLAN is a virtual bridge that has its own bridge ID and configurable STP parameters, such as protocol, priority, hello time, max-age, and forward delay.

- When operating in per-VLAN mode, 802.1Q tagged ports participate in an 802.1Q Spanning Tree instance that allows the Spanning Tree to extend across tagged VLANs. As a result, a tagged port can participate in more than one Spanning Tree instance; one for each VLAN that the port carries.
• If a VLAN contains both fixed and tagged ports and the switch is operating in per-VLAN Spanning Tree mode, then a hybrid of the two Spanning Tree instances (single and 802.1Q) is applied. If a VLAN appears as a tag on a port, then the BPDU for that VLAN are also tagged. However, if a VLAN appears as the configured default VLAN for the port, then BPDU are not tagged and the single Spanning Tree instance applies.

• Regardless of which mode the switch is running in, it is possible to administratively disable the Spanning Tree status for an individual VLAN (see Chapter 5, “VLAN Management Commands”).

**Note.** Active ports associated with such a VLAN are excluded from any Spanning Tree calculations and remain in a forwarding state.

**Examples**

--> spantree mode flat
--> spantree mode per-vlan

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **spantree protocol**
  Selects the Spanning Tree protocol for the specified instance.

- **spantree bpdu-switching**
  Enables the switching of Spanning Tree BPDU on a VLAN that has Spanning Tree disabled.

- **show spantree**
  Displays VLAN Spanning Tree parameter values.

**MIB Objects**

- **vStpTable**
  - **vStpNumber**
  - **vStpMode**
**spantree protocol**

Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance.

```
spantree [cist | vlan vlan_id] protocol {stp | rstp | mstp}
```

### Syntax Definitions

- **cist**: The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
- **vlan_id**: An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
- **stp**: IEEE 802.1D standard Spanning Tree Algorithm and Protocol.
- **rstp**: IEEE 802.1W Rapid Spanning Tree Protocol.
- **mstp**: IEEE 802.1Q 2005 Multiple Spanning Tree Protocol. This protocol is not supported on a per-VLAN basis.

### Defaults

By default, the Spanning Tree protocol is set to RSTP.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cist</td>
<td>vlan vlan_id</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If the optional **cist** or **vlan** parameter is not specified with this command, the protocol is set for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active.

**Note.** Selecting MSTP is only an option for the flat mode CIST instance and is required to configure Multiple Spanning Tree Instances (MSTI).

- MSTP is only active when the switch is operating in the flat Spanning Tree mode. STP and RSTP are active when the switch is operating in either the flat or per-VLAN Spanning Tree mode.
- Deleting all existing MSTIs is required before changing the protocol from MSTP to STP or RSTP.
**Note.** When the protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. However, if the path cost mode was set to 32-bit prior to the protocol change, the path cost is *not* reset to the default value. See the `spantree path-cost-mode` command page for more information.

**Examples**

-> spantree protocol mstp  
-> spantree cist protocol mstp  
-> spantree vlan 5 protocol rstp

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **spantree mode**  
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- **show spantree**  
  Displays the Spanning Tree instance configuration.

**MIB Objects**

- vStpInsTable
  - vStpInsNumber
  - vStpInsMode
  - vStpInsProtocolSpecification
**spantree vlan admin-state**

Enables or disables the Spanning Tree status for a VLAN.

```
spantree vlan vlan_id [-vlan_id2] admin-state {enable | disable}
```

### Syntax Definitions

- `vlan_id[-vlan_id2]`: An existing VLAN ID number. Use a hyphen to specify a range of VLANs (10-15).
- `enable`: Enables Spanning Tree for the specified VLAN.
- `disable`: Disables Spanning Tree for the specified VLAN.

### Defaults

By default, the Spanning tree status is enabled for a VLAN instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

VLAN Spanning Tree instances are only active when the switch is running in the per-VLAN mode. However, configuring the VLAN Spanning Tree status is allowed in both modes (per-VLAN and flat).

### Examples

- `-> spantree vlan 850-900 admin-state enable`
- `-> spantree vlan 720-750 admin-state disable`
- `-> spantree vlan 500 admin-state disable`

### Release History

Release 7.1.1; command introduced.
Related Commands

- **vlan**
  Creates a VLAN.

- **show vlan**
  Displays a list of existing VLANs.

- **show vlan members**
  Displays VLAN port assignments.

MIB Objects

- **vlanTable**
  - **vlanNumber**
  - **vlanAdmStatus**
  - **vlanOperStatus**
  - **vlanStatus**
spantree mst region name

Defines the name for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

no spantree mst region name

Syntax Definitions

name

An alphanumeric string. Use quotes around string if the name contains multiple words with spaces between them (for example, “ALE Marketing”).

Defaults

By default, the MST region name is left blank.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the MST region name.

Note. It is not necessary to specify the region name to remove it.

- To change the existing region, use this command with a string value that is different than the existing region name.

- Specifying an MST region name is allowed regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values, such as region name, only apply when the switch is operating in the flat Spanning Tree mode and using MSTP.

Examples

- > spantree mst region name SalesRegion
- > spantree mst region name "ALE Marketing"
- > no spantree mst region name
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mst region revision-level`  Defines the revision level for an MST region.
- `spantree mst region max-hops`  Defines the maximum number of hops for the MST region.
- `spantree msti`  Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
- `spantree msti vlan`  Defines an association between a range of VLANs and a single MSTI.

**MIB Objects**

- `vStpMstRegionTable`
  - `vStpMstRegionNumber`
  - `vStpMstRegionConfigName`
spantree mst region revision-level

Defines the revision level for a Multiple Spanning Tree (MST) region. One of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

\[
\text{spantree mst region revision-level} \ rev\_level
\]

### Syntax Definitions

- **rev_level**: A numeric value that identifies the MST region revision level for the switch.

### Defaults

By default, the MST revision level is set to zero.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

An MST region revision level can be assigned to the MST region regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values, such as revision level, only apply when the switch is operating in the flat Spanning Tree mode, using the MSTP.

### Examples

- `-> spantree mst region revision-level 1000`
- `-> spantree mst region revision-level 2000`

### Release History

Release 7.1.1; command introduced.
Related Commands

- `spantree mst region name` Defines the name for an MST region.
- `spantree mst region max-hops` Defines the maximum number of hops for the MST region.
- `spantree msti` Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.
- `spantree msti vlan` Defines an association between a range of VLANs and a single MSTI.

MIB Objects

- `vStpMstRegionTable`
  - `vStpMstRegionNumber`
  - `vStpMstRegionConfigRevisionLevel`
**spantree mst region max-hops**

Configures the maximum number of hops that are authorized to receive Multiple Spanning Tree (MST) regional information. Use this command to assign the maximum number of hops a BPDU is allowed to traverse, before it is discarded and related information is aged out.

**Syntax Definitions**

*max_hops*  
A numeric value that designates the maximum number of hops.

**Defaults**

By default, the maximum number of hops is set to 20.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The value configured with this command is a regional value that applies to all instances and is used to determine the size of the region.

- The maximum hop count value is the initial value of the “remaining hops” parameter in the MST BPDU that originates from the bridge that is serving as the root bridge for the region. Each bridge that in turn receives the MST BPDU decrements the “remaining hops” count value by one and passes the new value along to the next bridge. When the count reaches 0, the BPDU is discarded.

- Specifying an MST maximum hop count is allowed regardless of which Spanning Tree operating mode or protocol is currently active on the switch. However, MST configuration values only apply when the switch is operating in the flat Spanning Tree mode and using the MSTP.

**Examples**

```
-> spantree mst region max-hops 40
```

**Release History**

Release 7.1.1; command introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>spantree mst region name</code></td>
<td>Defines the name for an MST region.</td>
</tr>
<tr>
<td><code>spantree mst region revision-level</code></td>
<td>Defines the revision level for an MST region.</td>
</tr>
<tr>
<td><code>spantree msti</code></td>
<td>Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.</td>
</tr>
<tr>
<td><code>spantree msti vlan</code></td>
<td>Defines an association between a range of VLANs and a single MSTI.</td>
</tr>
</tbody>
</table>

### MIB Objects

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vStpMstRegionTable</td>
<td></td>
</tr>
<tr>
<td>vStpMstRegionNumber</td>
<td></td>
</tr>
<tr>
<td>vStpMstRegionMaxHops</td>
<td></td>
</tr>
</tbody>
</table>
**spantree msti**

Defines a Multiple Spanning Tree Instance (MSTI) number. This number identifies an association between a range of VLANs and a single Spanning Tree instance. In addition, it is possible to assign an optional name to the MSTI for further identification.

```
spantree msti msti_id [name name]
no spantree msti msti_id [name]
```

**Syntax Definitions**

- **msti_id**
  - A numeric MSTI ID number. A range of VLANs is associated to an MSTI ID number.
- **name**
  - An alphanumeric string. Use quotes around string if the name contains multiple words with spaces between them (for example, “ALE Marketing”).

**Defaults**

By default, a flat mode Common and Internal Spanning Tree (CIST) instance always exists. The MSTI ID number for this instance is 0.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the MSTI from the switch configuration.
- Use the **no** form of this command along with the **name** parameter to remove the optional MSTI name from the specified instance. The instance itself is not removed; only the name.
- There is always one CIST per switch. Initially all VLANs are associated with the CIST instance.
- Creating an MSTI is allowed when the switch is operating in either the per-VLAN or flat Spanning Tree mode, as long as MSTP is the selected flat mode protocol. The MSTI configuration, however, is not active unless the switch is running in the flat mode.

**Examples**

```
-> spantree msti 10
-> spantree msti 20 name BldgOneST10
-> no spantree msti 20 name
-> no spantree msti 10
```
Release History

Release 7.1.1; command introduced.

Related Commands

- `spantree mst region name`  Defines the name for an MST region.
- `spantree mst region revision-level`  Defines the revision level for an MST region.
- `spantree mst region max-hops`  Defines the maximum number of hops for the MST region.
- `spantree msti vlan`  Defines an association between a range of VLANs and a single MSTI.

MIB Objects

- `vStpMstInstanceTable`
  - `vStpMstInstanceNumber`
  - `vStpMstInstanceName`
  - `vStpMstInstanceVlanBitmapAddition`
  - `vStpMstInstanceVlanBitmapDeletion`
  - `vStpMstInstanceVlanBitmapState`
**spantree msti vlan**

Defines an association between a range of VLANs and a single Multiple Spanning Tree Instance (MSTI). The MSTI-to-VLAN mapping created with this command is one of three attributes (name, revision level, and a VLAN to MST instance association table) that defines an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same attribute values are all considered part of the same MST region. Currently each switch can belong to one MST region at a time.

```
spantree msti msti_id vlan vlan_id[,-vlan_id2]
```

```
no spantree msti msti_id vlan vlan_id[,-vlan_id2]
```

**Syntax Definitions**

- `msti_id`: A numeric MSTI identification number. A range of VLANs are associated to an MSTI ID number.
- `vlan_id[,-vlan_id2]`: A VLAN ID number. Use a hyphen to specify a range of VLAN IDs (for example, `vlan 10-15`).

**Defaults**

By default, all VLANs are associated with the flat mode Common and Internal Spanning Tree (CIST) instance, which is also known as MSTI 0.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a VLAN or a range of VLANs from the specified MSTI association.

- Note that the VLAN ID specified with this command does not have to already exist in the switch configuration. This command maps VLAN IDs to MSTIs, but does not create VLANs.

- A VLAN is associated with only one MSTI at a time, but it is possible to move a VLAN from one MSTI to another. In addition, it is also possible to assign only one VLAN to an MSTI; a range of VLANs is not required.

- To associate multiple VLANS in a single command, use a hyphen to specify a range of VLAN IDs and a space to separate multiple VLAN IDs and/or ranges (for example 100-115 122 135 200-210).

- Configuring an MSTI-to-VLAN mapping is allowed when the switch is operating in either the per-VLAN or flat Spanning Tree mode, as long as MSTP is the selected flat mode protocol. The MSTI configuration, however, is not active unless the switch is running in the flat mode.
**Examples**

-> `spantree msti 10 vlan 100-115`
-> `spantree msti 20 vlan 122`
-> `no spantree msti 10 vlan 100-115`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mst region name`  
  Defines the name for an MST region.
- `spantree mst region revision-level`  
  Defines the revision level for an MST region.
- `spantree mst region max-hops`  
  Defines the maximum number of hops for the MST region.
- `spantree msti`  
  Defines a MSTI number that identifies an association between a range of VLANs and a Spanning Tree instance.

**MIB Objects**

- `vStpMstVlanAssignmentTable`
  - `vStpMstVlanAssignmentVlanNumber`
  - `vStpMstVlanAssignmentEntry`
  - `vStpMstVlanAssignmentMstiNumber`
**spantree priority**

Configures the bridge priority value for the Common and Internal Spanning Tree (CIST) instance, a Multiple Spanning Tree Instance (MSTI), or a VLAN instance. This command is also used to configure the priority value for a port or link aggregate associated with the CIST, an MSTI, or a VLAN.

```
spantree [cist | msti msti_id | vlan vlan_id] [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] priority priority
```

**Syntax Definitions**

- **cist**: The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
- **msti_id**: An existing MSTI ID number. If MSTI 0 is specified, the priority applies to the CIST instance. This parameter is configurable in both modes (flat or per-VLAN) but only if the flat mode protocol is set to MSTP.
- **vlan_id**: An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **priority**: A bridge or port priority value. The valid range for the bridge priority is 0–65535. The valid range for the port priority is 0–15. If MSTP is the active flat mode protocol, enter a value that is a multiple of 4096 (for example, 4096, 8192, 12288).

**Defaults**

- By default, the bridge priority value is set to 32768 for the CIST, an MSTI, and a VLAN instance.
- By default, the port or link aggregate priority value is set to 7.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cist</td>
<td>msti msti_id</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- The bridge priority is used to determine which bridge the Spanning Tree algorithm designates as the root bridge. The port priority value is used to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge.

- The lower the bridge or port priority number assigned, the higher the priority that is associated with the bridge or port.

- If none of the optional instance parameters (`cist`, `msti`, or `vlan`) or `port` and `linkagg` parameters are specified with this command, the bridge priority is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.

- Although the `cist`, `msti`, and `vlan` parameters are configurable in both the flat and per-VLAN mode, the specified priority values are not applied unless the supporting mode (flat for CIST/MSTI or per-VLAN for a VLAN instance) is active.

- To configure the bridge priority with this command, specify the instance (`cist`, `msti`, or `vlan`) and the priority value; do not specify a port number or link aggregate ID.

- The bridge priority value for an MSTI is calculated by adding the configured priority value to the Spanning Tree instance number. For example, if the priority value of MSTI 10 equals 32768 (the default), then the Spanning Tree priority value advertised for this instance is 32770 (32768 + 10).

- When the protocol is changed to/from MSTP, the bridge priority for the flat mode CIST instance is reset to the default value.

- The bridge priority specifies the priority value for the first two octets of the Bridge ID (eight octets long). The remaining six octets of the Bridge ID contain a dedicated bridge MAC address. In regards to the priority for an MSTI, only the four most significant bits are used.

- To configure the port priority with this command, specify the instance (`cist`, `msti`, or `vlan`), a port number or link aggregate ID that is associated with that instance, and the priority value.

- The port priority value configured with this command is only applied to the specified instance. As a result, a single port can have different priority values for each instance. For example, in flat mode, port 1/24 can have a priority value of 7 for MSTI 2 and a priority value of 5 for MSTI 3.

- The port priority specifies the value of the priority field contained in the first byte of the port ID. The second byte contains the physical switch port number.

Examples

The following command examples set the bridge priority for the specified instance:

```
-> spantree priority 8192
-> spantree cist priority 8192
-> spantree vlan 2 priority 32679
-> spantree msti 1 priority 2500
ERROR: Valid bridge priority values are multiples of 4096: 0, 4096, 8192, 12288, 16384 ... 61440
-> spantree msti 1 priority 8192
```

The following command examples set the port priority for the specified instance:

```
-> spantree port 1/10 priority 10
-> spantree cist port 1/10 priority 10
-> spantree cist linkagg 10 priority 1
-> spantree vlan 200 port 2/1 priority 15
-> spantree vlan 2 linkagg 5 priority 2
```
Distributed Spanning Tree Commands

-> spantree msti 2 port 1/24 priority 5
-> spantree msti 3 linkagg 6-8 priority 10

Release History
Release 7.1.1; command introduced.

Related Commands

spantree mode  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

show spantree  Displays the Spanning Tree instance configuration.

show spantree ports  Displays the Spanning Tree port configuration.

MIB Objects

vStpInsTable
  vStpInsNumber
  vStpInsMode
  vStpInsPriority
  vStpInsBridgeAddress
spantree hello-time

Configures the Spanning Tree hello time value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN mode VLAN instance. This value specifies the amount of time, in seconds, between each transmission of a BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root.

`spantree [cist | vlan vlan_id] hello-time seconds`

**Syntax Definitions**

- **cist**: The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).
- **vlan_id**: An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).
- **seconds**: Specifies the Hello time value in seconds. The valid range is 1–10.

**Defaults**

By default, the bridge hello time value is set to 2 seconds.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cist</td>
<td>cist</td>
</tr>
<tr>
<td>vlan_id</td>
<td>vlan_id</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Lowering the Hello Time interval improves the robustness of the Spanning Tree Algorithm. Increasing the Hello Time interval lowers the overhead of the Spanning Tree Algorithm.

- If the optional `cist` or `vlan` parameter is not specified with this command, the hello time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.

- Although the `cist` and `vlan` parameters are configurable in both the flat and per-VLAN mode, the specified hello time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.

- Note that for Multiple Spanning Tree Instances (MSTI), the hello time value is inherited from the CIST instance and is not a configurable parameter.
Examples

-> spantree hello-time 5
-> spantree cist hello-time 5
-> spantree vlan 10 hello-time 3

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode
Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

show spantree
Displays the Spanning Tree instance configuration.

MIB Objects

vStpInsTable
  vStpInsNumber
  vStpInsMode
  vStpInsBridgeHelloTime
**spantree max-age**

Configures the bridge maximum age time value for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN mode VLAN instance. This value is the amount of time, in seconds, that the Spanning Tree Protocol information learned from the network on any port is retained. This information is discarded when it ages beyond the maximum age value.

`spantree [cist | vlan vlan_id] max-age seconds`

**Syntax Definitions**

- **cist**
  - The CIST instance (also known as MSTI 0). This parameter is configurable in both modes (flat or per-VLAN).

- **vlan_id**
  - An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).

- **seconds**
  - Max-age time in seconds. The valid range is 6–40.

**Defaults**

By default, the bridge maximum age time value is set to 20 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A low maximum age time causes the Spanning Tree Algorithm to reconfigure more often.

- If the optional **cist** or **vlan** parameter is not specified with this command, the maximum age time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.

- Although the **cist** and **vlan** parameters are configurable in both the flat and per-VLAN mode, the specified maximum age time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.

- Note that for Multiple Spanning Tree Instances (MSTI), the maximum age time value is inherited from the CIST instance and is not a configurable parameter.
**Examples**

-> spantree max-age 10  
-> spantree cist max-age 10  
-> spantree vlan 10 max-age 30

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **spantree mode**
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- **show spantree**
  Displays the Spanning Tree instance configuration.

**MIB Objects**

- vStpInsTable
  - vStpInsNumber
  - vStpInsBridgeMaxAge
**spantree forward-delay**

Configures the bridge forward delay time for the flat mode Common and Internal Spanning Tree (CIST) instance or for a per-VLAN mode VLAN instance. This value is the amount of time, in seconds, that determines how fast a port changes its Spanning Tree state until it reaches a forwarding state. The forward delay time specifies how long a port stays in the listening and learning states, which precede the forwarding state.

```plaintext
spantree [cist | vlan vlan_id] forward-delay seconds
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cist</td>
<td>The CIST instance (also known as MST1 0). This parameter is configurable in both modes (flat or per-VLAN).</td>
</tr>
<tr>
<td>vlan_id</td>
<td>An existing VLAN ID number. This parameter is configurable in both modes (flat or per-VLAN).</td>
</tr>
<tr>
<td>seconds</td>
<td>Forward delay time, in seconds. The valid range is 4–30.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, the bridge forward delay time value is set to 15 seconds.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cist</td>
<td>vlan vlan_id</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A low forward delay time can cause temporary loops in the network, because data may get forwarded before the reconfiguration message has reached all nodes on the network.
- The forward delay time is also used to age out all dynamic MAC address entries in the forwarding table (MAC address table) when a topology change occurs.
- If the optional `cist` or `vlan` parameter is not specified with this command, the forward delay time is configured for the CIST instance by default. This is true regardless of which mode (flat or per-VLAN) is active for the switch.
- Although the `cist` and `vlan` parameters are configurable in both the flat and per-VLAN mode, the specified forward delay time value is not applied unless the supporting mode (flat for CIST or per-VLAN for a VLAN instance) is active.
- Note that for Multiple Spanning Tree Instances (MSTI), the forward delay time is inherited from the CIST instance and is not a configurable parameter.

**Examples**

- `-> spantree forward-delay 30`
- `-> spantree cist forward-delay 30`
- `-> spantree vlan 5 forward-delay 10`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mode` Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
- `show spantree` Displays the Spanning Tree instance configuration.

**MIB Objects**

- `vStpInsTable`
  - `vStpInsNumber`
  - `vStpInsMode`
  - `vStpInsBridgeForwardDelay`
spantree bpdu-switching

Enables or disables the switching of Spanning Tree BPDU for VLAN and CIST instances if the switch is running in the per-VLAN mode.

`spantree {vlan vlan_id | cist} bpdu-switching {enable | disable}`

### Syntax Definitions

- **vlan_id**: An existing VLAN ID number.
- **enable**: Enables BPDU switching for the specified instance.
- **disable**: Disables BPDU switching for the specified instance.

### Defaults

By default, BPDU switching is disabled for VLAN or CIST instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Specifying the BPDU switching status for a VLAN does not depend on the current VLAN Spanning Tree status. For example, setting the BPDU switching status to enabled is allowed on a VLAN that also has Spanning Tree enabled.

- Use the `vlan` parameter along with the `vlan_id` to enable or disable BPDU switching for a particular VLAN.

- Use the `cist` parameter to enable or disable BPDU switching for the CIST instance.

### Examples

- `spantree mode flat`
- `spantree bpdu-switching enable`
- `spantree bpdu-switching disable`
- `spantree cist bpdu-switching enable`
- `spantree cist bpdu-switching disable`

- `spantree mode per-vlan`
- `spantree vlan 10 bpdu-switching enable`
- `spantree vlan 10 bpdu-switching disable`
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `vlan members untagged` Enables or disables Spanning Tree instance for the specified VLAN.
- `show spantree` Displays VLAN Spanning Tree parameter values.

**MIB Objects**

- `vStpInsTable`
  - `vStpInsBpduSwitching`
spantree path-cost-mode

Configures the automatic selection of a 16-bit path cost for STP/RSTP ports and a 32-bit path cost for MSTP ports or sets all path costs to use a 32-bit value.

spantree path-cost-mode {auto | 32bit}

Syntax Definitions

auto The port path cost value is automatically set depending on which protocol is active on the switch (32-bit for MSTP, 16-bit for STP/RSTP).

32bit Specifies that a 32-bit value is used for the port path cost value regardless of which protocol is active on the switch.

Defaults

By default, the path cost mode is set to auto.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- All path cost values, except those for MSTIs, are reset to the default path cost value when this mode is changed.
- When connecting a switch running in the 32-bit path cost mode to a switch running in the 16-bit mode, the 32-bit switch has a higher path cost value and thus an inferior path cost to the 16-bit switch. To avoid this, use the spantree path-cost-mode command to change the 32-bit switch to a 16-bit switch.
- Note that when the protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values. The exception to this is if the path cost mode is set to 32-bit prior to the protocol change, the path cost is not reset to its default value.

Examples

- `spantree path-cost-mode 32bit`
- `spantree path-cost-mode auto`

Release History

Release 7.1.1; command introduced.
Related Commands

**spantree protocol**  
Configures the protocol for the flat mode CIST instance or a per-VLAN mode VLAN instance.

MIB Objects

vStpBridge  
vStpPathCostMode
**spantree pvst+compatibility**

Enables or disables PVST+ mode on the switch, port or link aggregate enabling them to operate with Cisco switches.

```plaintext
spantree pvst+compatibility {port chassis/slot/port | linkagg agg_id} {enable | disable | auto}
```

### Syntax Definitions

- **chassis**
  The chassis identifier.
- **slot/port[-port2]**
  The slot number and port number of the physical port.
- **agg_id[-agg_id2]**
  The link aggregate ID number.
- **enable**
  Enables the PVST+ mode.
- **disable**
  Disables the PVST+ mode.
- **auto**
  IEEE BPDUs are used until a PVST+ BPDU is detected.

### Defaults

PVST+ is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- In order to handle PVST+ mode, the ports must be configured in per-VLAN mode.
- Specify `pvst+compatibility enable` to enable all the ports on the switch to handle PVST+ BPDUs.
- Initially, a port sends or receive IEEE BPDUs. Once a PVST+ BPDU is received, the port sends and receives only PVST+ BPDUs for tagged VLANs and IEEE BPDUs for default VLANs.

### Examples

```plaintext
-> spantree pvst+compatibility enable
-> spantree pvst+compatibility disable
-> spantree port 1/3 pvst+compatibility enable
-> spantree port 2/2 pvst+compatibility auto
-> spantree linkagg 2 pvst+compatibility enable
```

### Release History

Release 7.1.1; command introduced.
Related Commands

- **show spantree**: Displays Spanning Tree bridge information for all flat mode Common and Internal Spanning Tree (CIST) instance and per-VLAN mode VLAN instance.
- **show spantree ports**: Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance or a per-VLAN mode VLAN instance.
- **show spantree cist ports**: Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance.
- **show spantree msti ports**: Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

MIB Objects

- vStpPortConfigPVST
- vStpPortConfigStatePVST
- vStpBridgeModePVST
**spantree auto-vlan-containment**

Enables or disables Auto VLAN Containment (AVC). When enabled, AVC prevents a port that has no VLANs mapped to an Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Such ports are automatically assigned an infinite path cost value to make them an inferior choice for root port.

```
spantree [msti msti_id] auto-vlan-containment {enable | disable}
```

**Syntax Definitions**

- `msti_id` An existing MSTI ID number. A range of VLANs are associated to an MSTI ID number.
- `enable` Enables automatic VLAN containment.
- `disable` Disables automatic VLAN containment.

**Defaults**

By default, automatic VLAN containment is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The AVC feature is not active for any MSTI until it is globally enabled. To globally enable this feature, use the `spantree auto-vlan-containment` command but do not specify an `msti_id`.
- When AVC is globally enabled, it is active for all MSTIs. To disable AVC for a single instance, specify the `msti_id` for the instance and use the `disable` form of this command.
- Use the `enable` form of this command and specify an `msti_id` to enable AVC for an instance that was previously disabled.
- An administratively set port path cost takes precedence and prevents AVC configuration of the path cost. However, if the port path cost is administratively set to zero, then the path cost is reset to the default value.
- Note that when AVC is disabled, a port assigned to a VLAN that is not mapped to a specific instance, can become the root port for that instance and cause a loss of connectivity between other VLANs.
- AVC does not have any effect on root bridges.
**Examples**

-> spantree auto-vlan-containment enable  
-> spantree auto-vlan-containment disable  
-> spantree msti 1 auto-vlan-containment disable  
-> spantree msti 1 auto-vlan-containment enable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**show spantree msti ports**  
Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

**MIB Objects**

vStpInsTable
  vStpInsAutoVlanContainment
vStpBridge
  vStpBridgeAutoVlanContainment
**spantree cist**

Enables or disables the Spanning Tree status on a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance.

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} {enable | disable}
```

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port[-port2]`: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id[-agg_id2]`: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `enable`: Enables Spanning Tree on the specified port for the CIST instance.
- `disable`: Disables Spanning Tree on the specified port for the CIST instance.

**Defaults**

By default, the Spanning Tree status is enabled on eligible ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 \ V72/C32</th>
<th>6900 \ X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the CIST instance regardless of which Spanning Tree operating mode (flat or per-VLAN) or protocol is active for the switch.

- If the switch is running in per-VLAN mode when this command is used, the Spanning Tree status configured for the port is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.

- When the Spanning Tree status is disabled on a port, the port is set to a forwarding state for the specified instance.

- Physical ports that are reserved for link aggregation do not participate in the Spanning Tree Algorithm. Instead, the algorithm is applied to the aggregate logical link (virtual port) that represents a collection of physical ports.

**Examples**

```
-> spantree cist port 4/1 enable
-> spantree cist port 4/2-5 disable
```
- spantree cist linkagg 16 disable
- spantree cist linkagg 22-26 enable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **spantree mode**
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- **spantree vlan**
  Configures the Spanning Tree status on a port or a link aggregate of ports for a VLAN instance.

**MIB Objects**

- vStpInsPortTable
  - vStpInsPortNumber
  - vStpInsPortEnable
**spantree vlan**

Enables or disables the Spanning Tree status on a port or a link aggregate of ports for the specified VLAN instance.

`spantree vlan vlan_id [-vlan2] [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] {enable | disable}`

**Syntax Definitions**

- `vlan_id`  
  An existing VLAN ID number.
- `chassis`  
  The chassis identifier.
- `slot/port[-port2]`  
  The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id[-agg_id2]`  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `enable`  
  Enables Spanning Tree on the specified port for the specified instance.
- `disable`  
  Disables Spanning Tree on the specified port for the specified instance.

**Defaults**

By default, the Spanning Tree status is enabled on eligible ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the specified VLAN instance regardless of which Spanning Tree operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the Spanning Tree status configured for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.
- When the Spanning Tree status is disabled on a port, the port is set to a forwarding state for the specified instance.
- If STP is disabled on a VLAN in the per-VLAN mode, the port Spanning Tree status is ignored and all active ports associated with the VLAN are put in a forwarding state and not included in the Spanning Tree Algorithm. Note that when this occurs, ports will *not* bridge BPDU unless the BPDU switching status for the VLAN is enabled.
Physical ports that are reserved for link aggregation do not participate in the Spanning Tree Algorithm. Instead, the algorithm is applied to the aggregate logical link (virtual port) that represents a collection of physical ports.

**Examples**

- `-> spantree vlan 2 port 4/1 enable`
- `-> spantree vlan 2 port 4/2-5 disable`
- `-> spantree vlan 3 linkagg 16 disable`
- `-> spantree vlan 3 linkagg 22-25 disable`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mode` Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
- `spantree cist` Configures the Spanning Tree status on a port or an aggregate of ports for the CIST instance when the switch is operating in either the per-VLAN or flat mode.
- `spantree vlan admin-state` Enables or disables Spanning Tree instance for the specified VLAN.
- `spantree bpdu-switching` Enables or disables the switching of Spanning Tree BPDU for all VLAN instances if the switch is running in the per-VLAN mode.

**MIB Objects**

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortEnable`
**spantree cist path-cost**

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} path-cost path_cost
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `path_cost` Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

**Defaults**

By default, the path cost is set to zero.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the port path cost value for the CIST instance regardless of which operating mode (flat or per-VLAN) or protocol is active for the switch.

- If the switch is running in per-VLAN mode when this command is used, the specified path cost value is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.

- Note that when the Spanning Tree protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.

- Use the `spantree path-cost-mode` command to automatically select the path cost value based on the active Spanning Tree protocol (16-bit for STP and RSTP, 32-bit for MSTP) or to use a 32-bit path cost value regardless of which protocol is active.

- If the `path_cost` is set to zero, there are recommended 16-bit and 32-bit values which are used by default depending on the link speed. Refer to the “Configuring Spanning Tree Parameters” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide for a list of values.
Examples

- `spantree cist port 4/1 path-cost 19`
- `spantree cist port 4/2-5 path-cost 19`
- `spantree cist linkagg 16 path-cost 12000`
- `spantree cist linkagg 17-20 path-cost 12000`

Release History

Release 7.1.1; command introduced.

Related Commands

- `spantree mode` Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
- `spantree path-cost-mode` Selects a 32-bit or automatic path cost mode for the switch.
- `spantree msti path-cost` Configures the Spanning Tree path cost value for a port or a link aggregate of ports for an MSTI.
- `spantree vlan path-cost` Configures the Spanning Tree path cost value for a port or a link aggregate of ports for a VLAN instance.

MIB Objects

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortPathCost`
**spantree msti path-cost**

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the specified flat mode Multiple Spanning Tree Instance (MSTI). This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

**spantree msti msti_id {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} path-cost path_cost**

**Syntax Definitions**

- **msti_id**
  An existing MSTI ID number. If MSTI 0 is specified, the priority applies to the CIST instance.

- **chassis**
  The chassis identifier.

- **slot/port[-port2]**
  The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

- **agg_id[-agg_id2]**
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **path_cost**
  Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

**Defaults**

By default, the path cost is set to zero.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the specified MSTI regardless of which operating mode (flat or per-VLAN) is active for the switch. However, if MSTP is not the selected flat mode protocol, the path cost value for any MSTI is not configurable.

- Note that if zero is entered for the *msti_id* value, the specified path cost value is applied to the CIST instance.

- Note that when the Spanning Tree protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.

- The path cost value configured with this command is only applied to the specified instance. As a result, a single port can have a different path cost for each instance. For example, in flat mode, port 1/24 can have a path cost of 20000 for MSTI 2 and a path cost of 35000 for MSTI 3.
• If the switch is running in per-VLAN mode when this command is used, the specified path cost value is not active for the specified MSTI until the operating mode for the switch is changed to the flat mode.

• When MSTP is the active protocol on the switch, only a 32-bit path cost value is used. Using a 16-bit path cost value is not an option.

• If the path_cost is set to zero, there are recommended 16-bit and 32-bit values which are used by default depending on the link speed. Refer to the “Configuring Spanning Tree Parameters” chapter for a list of values.

**Examples**

```
-> spantree msti 0 port 4/1 path-cost 35000
-> spantree msti 0 port 1/20-24 path-cost 12000
-> spantree msti 2 linkagg 10 path-cost 20000
-> spantree msti 2 linkagg 10-12 path-cost 65000
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mode` Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
- `spantree cist path-cost` Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the CIST instance.
- `spantree vlan path-cost` Configures the Spanning Tree path cost value for a port or a link aggregate of ports for a VLAN instance.

**MIB Objects**

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortPathCost`
spantree vlan path-cost

Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the specified VLAN instance. This value is the contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops.

```
spantree vlan vlan_id {port chassis/slot/port|-port2] | linkagg agg_id[-agg_id2]} path-cost path_cost
```

**Syntax Definitions**

- `vlan_id`: An existing VLAN ID number.
- `chassis`: The chassis identifier.
- `slot/port|-port2]`: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id][-agg_id2]`: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `path_cost`: Path cost value. The valid range is 0 - 65535 for 16-bit, 0–200000000 for 32-bit.

**Defaults**

By default, the path cost is set to zero.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the flat mode when this command is used, the specified path cost for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.

- Note that when the Spanning Tree protocol is changed to/from MSTP, the bridge priority and port path cost values for the flat mode CIST instance are reset to their default values.

- Use the `spantree path-cost-mode` command to automatically select the path cost value based on the active Spanning Tree protocol (16-bit for STP and RSTP, 32-bit for MSTP) or to use a 32-bit path cost value regardless of which protocol is active.
• If the `path_cost` is set to zero, there are recommended 16-bit and 32-bit values which are used by default depending on the link speed. Refer to the “Configuring Spanning Tree Parameters” chapter for a list of values.

**Examples**

- `spantree vlan 200 port 4/1 path-cost 4`
- `spantree vlan 200 port 4/2-5 path-cost 4`
- `spantree vlan 300 linkagg 16 path-cost 200000`
- `spantree vlan 500 linkagg 24-28 path-cost 20000`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mode`  
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- `spantree cist path-cost`  
  Configures the Spanning Tree path cost value for a port or a link aggregate of ports for the CIST instance.

- `spantree msti path-cost`  
  Configures the Spanning Tree path cost value for a port or a link aggregate of ports for an MSTI.

**MIB Objects**

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortPathCost`
**spantree cist mode**

Configures manual mode (forwarding or blocking) or dynamic mode to manage the state of a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST) instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} mode {forwarding | dynamic | blocking}
```

**Syntax Definitions**

- `chassis` The chassis identifier when running in virtual chassis mode.
- `slot/port[-port2]` The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `forwarding` Sets the port state to forwarding.
- `dynamic` Port state is determined by the Spanning Tree algorithm.
- `blocking` Sets the port state to blocking.

**Defaults**

By default, the port Spanning Tree mode is set to dynamic.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the port Spanning Tree mode for the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in per-VLAN mode when this command is used, the specified port mode is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree algorithm.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.
Examples

-> spantree cist port 4/1 mode forwarding
-> spantree cist port 4/2-5 mode forwarding
-> spantree cist linkagg 10 mode blocking
-> spantree cist linkagg 15-20 mode forwarding

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree loop-guard

Configures the Spanning Tree mode for a port or a link aggregate of ports for the specified VLAN instance.

MIB Objects

vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortManualMode
**spantree loop-guard**

Enables or disables the STP loop-guard on a port or link aggregate.

```
spantree {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} loop-guard {enable | disable}
```

### Syntax Definitions

- **chassis**
  
  The chassis identifier.

- **slot/port[-port2]**
  
  The slot number and port number of the physical port. Use a hyphen to specify a range of ports.

- **agg_id[-agg_id2]**
  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (example 10-20).

- **enable**
  
  Enables STP loop-guard.

- **disable**
  
  Disables STP loop-guard.

### Defaults

STP loop-guard is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When you enable loop-guard on a port, it is automatically applied to all the active instances or VLANs associated to the port.

- Loop-guard cannot be enabled on a port if root-guard is already enabled on the port or link aggregate related to the port. Root-guard must be disabled before configuring loop-guard. Similarly, when loop-guard configuration is enabled on a port or chassis, root-guard cannot be configured on the port/s.

- Loop-guard can be enabled on all types of ports including designated (forwarding), non-designated (alternate, secondary, or root) ports. However, STP loop-guard configuration does not affect designated ports. Hence, loop-guard is not effective when applied on designated ports.

- When loop-guard is enabled on root ports, they change to blocking mode when a loop-guard error occurs. In such an instance, the alternate or secondary ports takeover until the root port recovers from the error state.

- If a set of ports that are already blocked by loop-guard are grouped together to form a link aggregate, the new link aggregate gets a new designated role. The link aggregate can also obtain a forwarding state depending on the STP state.
• If a spanning tree channel is blocked by loop-guard and the channel breaks, spanning tree loses all the state information. The individual physical ports obtain the designated role, even if one or more of the links that formed the channel are unidirectional. New link aggregate might obtain a forwarding state but new port state is defined.

• The ports that are configured as fast-forwarding or edge-ports do not receive BPDUs. Loop-guard is not effective on such ports.

• Loop-guard error state is recovered when the administrative state of the port is enabled or disabled.

• When a VLAN is disabled, all the VLAN port associations recover from the error state.

• The loop-guard feature can be enabled on the ports that have STP (RSTP, MRSTP or MSTP) enabled.

• STP loop-guard on link aggregate protects all ports that are members of the link aggregation group.

Examples

-> spantree port 1/1/2 loop-guard enable
-> spantree linkagg 1 loop-guard enable
-> spantree port 1/1/2 loop-guard disable
-> spantree linkagg 1 loop-guard disable

Release History

Release 8.2.1; command introduced.

Related Commands

show spantree ports Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance or a 1x1 mode VLAN instance.

MIB Objects

vStpPortConfigTable
  vStpPortConfigIfIndex
  vStpPortConfigLoopGuard
**spantree vlan mode**

Configures Manual mode (forwarding or blocking) or Dynamic mode to manage the state of a port or a link aggregate of ports for the specified VLAN instance. Dynamic mode defers the management of the port state to the Spanning Tree algorithm.

```
spantree vlan vlan_id [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] mode {dynamic | blocking | forwarding}
```

**Syntax Definitions**

- `vlan_id`: An existing VLAN ID number.
- `chassis`: The chassis identifier when running in virtual chassis mode.
- `slot/port[-port2]`: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id[-agg_id2]`: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `dynamic`: Port state is determined by the Spanning Tree algorithm.
- `blocking`: Sets the port state to blocking.
- `forwarding`: Sets the port state to forwarding.

**Defaults**

By default, the port Spanning Tree mode is set to dynamic.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified mode for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.
- Ports manually configured to operate in a forwarding or blocking state do not participate in the Spanning Tree algorithm.
- When port state is manually set to forwarding or blocking, the port remains in that state until it is changed using this command.
**Examples**

-> `spantree vlan 255 port 4/1-4 mode forwarding`
-> `spantree vlan 355 port 1/24 mode dynamic`
-> `spantree vlan 450 linkagg 1 mode dynamic`
-> `spantree vlan 450 linkagg 1-5 mode dynamic`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mode` Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
- `spantree cist mode` Configures the Spanning Tree mode for a port or a link aggregate of ports for the CIST instance.

**MIB Objects**

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortManualMode`
**spantree cist connection**

Configures the connection type for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} connection {noptp | ptp | autoptp}
```

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port[-port2]`: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id[-agg_id2]`: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `noptp`: Defines port connection type as no point to point link.
- `ptp`: Defines port connection type as point to point link.
- `autoptp`: Specifies that switch software automatically defines connection type as point-to-point or no point-to-point.

**Defaults**

By default, the link connection type is set to auto point-to-point.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the port connection type for the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in per-VLAN mode when this command is used, the specified port connection type is not active for the CIST instance until the operating mode for the switch is changed to the flat mode.

- A port is considered connected to a point-to-point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port must run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point-to-point LAN segment.
• Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point-to-point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

**Examples**

`-> spantree cist port 7/24 connection noptp`
`-> spantree cist port 7/25-28 connection ptp`
`-> spantree cist linkagg 5-10 connection autoptp`
`-> spantree cist linkagg 5-10 connection autoptp`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **spantree mode**
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- **spantree cist admin-edge**
  Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.

- **spantree cist auto-edge**
  Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the flat mode CIST instance.

**MIB Objects**

- **vStpInsPortTable**
  - **vStpInsPortNumber**
  - **vStpInsPortAdminConnectionType**
  - **vStpInsPortOperConnectionType**
spantree vlan connection

Configures the connection type for a port or a link aggregate of ports for a VLAN instance.

```
spantree vlan vlan_id {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} connection {noptp | ptp | autoptp}
```

---

**Syntax Definitions**

- **vlan_id**: An existing VLAN ID number.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **noptp**: Defines port connection type as no point to point link.
- **ptp**: Defines port connection type as point to point link.
- **autoptp**: Specifies that switch software automatically defines connection type as point-to-point or no point-to-point.

---

**Defaults**

By default, the link connection type is set to auto point-to-point.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the flat mode when this command is used, the specified connection type for the port is not active for the specified VLAN instance until the operating mode for the switch is changed to the per-VLAN mode.

- A port is considered connected to a point-to-point LAN segment if the port belongs to a link aggregate of ports or if autonegotiation determines the port must run in full duplex mode or if full duplex mode was administratively set. Otherwise, the port is considered connected to a no point-to-point LAN segment.
• Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

Examples
-> spantree vlan 255 port 7/24 connection noptp
-> spantree vlan 255 port 7/25-27 connection ptp
-> spantree vlan 255 linkagg 3 connection autoptp
-> spantree vlan 255 linkagg 3-7 connection autoptp

Release History
Release 7.1.1; command introduced.

Related Commands
spantree mode Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch
spantree cist admin-edge Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
spantree cist auto-edge Configures whether or not Spanning Tree automatically determines the operational edge status of a port or an aggregate of ports for the flat mode CIST instance.

MIB Objects
vStpInsPortTable
   vStpInsPortNumber
   vStpInsPortAdminConnectionType
   vStpInsPortOperConnectionType
**spantree cist admin-edge**

Configures the administrative edge port status for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} admin-edge {enable | disable}
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **enable**
  - Enables the administrative edge port status for the specified port-CIST instance.

- **disable**
  - Disables the administrative edge port status for the specified port-CIST instance.

**Defaults**

By default, the administrative edge port status is disabled (off).

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the port connection type for the CIST instance regardless of which operating mode (flat or per-VLAN) is active on the switch.

- If the switch is running in the per-VLAN mode when this command is used, the specified edge port status is not active for the CIST instance until the switch is configured to run in the flat Spanning Tree mode.

- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (auto-edge) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.

- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as a point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
Configure ports that connect to a host (PC, workstation, server, and so on) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point-to-point connection type.

**Examples**

- `spantree cist linkagg 15 admin-edge enable`
- `spantree cist linkagg 4-10 admin-edge enable`
- `spantree cist port 8/25 admin-edge disable`
- `spantree cist port 2/2-5 admin-edge enable`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mode` Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
- `spantree vlan admin-edge` Configures the administrative edge port status for a port or a link aggregate of ports for a specific VLAN instance.
- `spantree cist auto-edge` Configures whether or not Spanning Tree automatically determines the operational edge status of a port or a link aggregate of ports for the flat mode CIST instance.
- `spantree vlan auto-edge` Configures whether or not Spanning Tree determines the operational edge port status for a port or a link aggregate of ports for the specified per-VLAN mode VLAN instance.

**MIB Objects**

- `vStpInsPortTable`
- `vStpInsPortNumber`
- `vStpInsPortAdminEdge`
**spantree vlan admin-edge**

Configures the administrative edge port status for a port or a link aggregate of ports for a VLAN instance.

```
spantree vlan vlan_id {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} admin-edge {enable | disable}
```

### Syntax Definitions

- **vlan_id**
  
  An existing VLAN ID number.

- **chassis**
  
  The chassis identifier.

- **slot/port[-port2]**
  
  The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

- **agg_id[-agg_id2]**
  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **enable**
  
  Enables the administrative edge port status for the specified port-VLAN instance.

- **disable**
  
  Disables the administrative edge port status for the specified port-VLAN instance.

### Defaults

By default, the administrative edge port status is disabled (off).

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

| 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | V72/C32 | 6900 | 6900 | X48C6/T48C6/ |
|------|------|------|--------|------|--------|------|------|---------|------|------|X48C4E/V48C8/ |
|      |      |      |        |      |        |      |      |         |      |      |C32E/T24C2/ |
|      |      |      |        |      |        |      |      |         |      |      |X24C2     |
| 6900 | V72/C32 |      | 6900 |      | 6900 |      |      | 9900    |      |      |          |
|      |        |      |      |      |      |      |      |         |      |      |          |
| Yes  | Yes    | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes     | Yes  | Yes  | Yes       |

### Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the flat mode when this command is used, the specified edge port status for the port is not active for the VLAN instance until the switch is configured to run in the per-VLAN Spanning Tree mode.

- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (**auto-edge**) is disabled for the port. However, if **auto-edge** is enabled for the port, then the administrative status is overridden.

- Rapid transition of a designated port to forwarding can only occur if the port connection type is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
• Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

**Examples**

-> spantree vlan 4 linkagg 15 admin-edge enable
-> spantree vlan 5 linkagg 12-14 admin-edge enable
-> spantree vlan 255 port 8/23 admin-edge disable
-> spantree vlan 3 port 2/2-5 admin-edge enable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**spantree mode**

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

**spantree cist admin-edge**

Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.

**spantree cist auto-edge**

Configures whether or not Spanning Tree automatically determines the operational edge status of a port or aggregate of ports for the flat mode CIST instance.

**spantree vlan auto-edge**

Configures whether or not Spanning Tree determines the operational edge port status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.

**MIB Objects**

vStpInsPortTable
vStpInsPortNumber
vStpInsPortAdminEdge
**spantree cist auto-edge**

Configures whether or not Spanning Tree automatically determines the operational edge port status of a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} auto-edge {enable | disable}
```

**Syntax Definitions**

- `chassis`  
  The chassis identifier.

- `slot/port[-port2]`  
  The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

- `agg_id[-agg_id2]`  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- `enable`  
  Spanning Tree automatically determines edge port status.

- `disable`  
  Spanning Tree does not automatically determine edge port status.

**Defaults**

By default, automatic edge port status configuration is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6450</th>
<th>6565</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the per-VLAN mode when this command is used, the specified edge port status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree mode.

- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (auto-edge) is disabled for the port. However, if auto-edge is enabled for the port, then the administrative status is overridden.

- Rapid transition of a designated port to forwarding can only occur if the connection type of the port is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.

- Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevents the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going
active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

**Examples**

```
-> spantree cist linkagg 15 auto-edge enable
-> spantree cist linkagg 10-12 auto-edge disable
-> spantree cist port 8/23 auto-edge disable
-> spantree cist port 2/2-5 auto-edge enable
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `spantree mode` Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.
- `spantree vlan auto-edge` Configures whether or not Spanning Tree determines the operational edge port status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.
- `spantree cist admin-edge` Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.
- `spantree vlan admin-edge` Configures the administrative edge port status for a port or aggregate of ports for a specific VLAN instance.

**MIB Objects**

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortAutoEdge`
spantree vlan auto-edge

Configures whether or not Spanning Tree determines the operational edge port status for a port or a link aggregate of ports for the specified per-VLAN mode VLAN instance.

```
spantree vlan vlan_id {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} auto-edge {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>An existing VLAN ID number.</td>
</tr>
<tr>
<td><code>chassis</code></td>
<td>The chassis identifier when running in virtual chassis mode.</td>
</tr>
<tr>
<td><code>slot/port[-port2]</code></td>
<td>The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).</td>
</tr>
<tr>
<td><code>agg_id[-agg_id2]</code></td>
<td>The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Spanning Tree automatically determines edge port status.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Spanning Tree does not automatically determine edge port status.</td>
</tr>
</tbody>
</table>

### Defaults

By default, automatic edge port status configuration is enabled (on).

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the flat mode when this command is used, the specified edge port status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.

- The administrative edge port status is used to determine if a port is an edge or non-edge port when automatic edge port configuration (auto-edge) is disabled for the port. However, if auto-edge is enabled for the port, then the administrative status is overridden.

- Rapid transition of a designated port to forwarding can only occur if the connection type of the port is defined as point to point or an edge port. Rapid transition of an alternate port role to a root port role is not affected by the port connection type definition.
• Configure ports that connect to a host (PC, workstation, server, and so on.) as edge ports to avoid unnecessary topology changes when these ports go active. This also prevent the flushing of learned MAC addresses on these ports if a topology change occurs as a result of another non-edge port going active. If an edge port receives a BPDU, it operationally reverts back to a no point to point connection type.

**Examples**

-> spantree vlan 255 port 8/23 auto-edge disable  
-> spantree vlan 4 port 2/2-10 auto-edge enable  
-> spantree vlan 100 linkagg 10 auto-edge disable  
-> spantree vlan 200 linkagg 1-5 auto-edge enable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **spantree mode**
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- **spantree cist auto-edge**
  Configures whether or not Spanning Tree automatically determines the operational edge status of a port or aggregate of ports for the flat mode CIST instance.

- **spantree cist admin-edge**
  Configures the administrative edge port status for a port or aggregate of ports for the CIST instance.

- **spantree vlan admin-edge**
  Configures the administrative edge port status for a port or aggregate of ports for a specific VLAN instance.

**MIB Objects**

- vStpInsPortTable
- vStpInsPortNumber
- vStpInsPortAutoEdge
spantree cist restricted-role

Configures the restricted role status for a port or a link aggregate of ports. Enabling this parameter blocks the port from becoming the Root Port, even if it is the most likely candidate for root. Once a root port is selected, the restricted port is selected as an Alternate Port.

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} {restricted-role | root-guard} {enable | disable}
```

### Syntax Definitions

- **chassis**
  
  The chassis identifier.

- **slot/port[-port2]**
  
  The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

- **agg_id[-agg_id2]**
  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **root-guard**
  
  Optional command syntax. Enter `root-guard` instead of restricted-role; both parameters specify the same functionality for this command.

- **enable**
  
  Enables the restricted role status for the specified port.

- **disable**
  
  Disables the restricted role status for the specified port.

### Defaults

By default, the restricted role status for the port is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When running in flat mode, this is a per-port setting and is applicable to any CIST or MSTI instances configured on that port.

- Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.

- Note that enabling the restricted role status for a port may impact connectivity within the network.

### Examples

- `-> spantree cist linkagg 15-20 restricted-role enable`
- `-> spantree cist linkagg 15-20 root-guard enable`
- `-> spantree cist port 8/23 restricted-role disable`
Distributed Spanning Tree Commands

spantree cist restricted-role

-> spantree cist port 1/1/4 root-guard enable
-> spantree cist port 8/24-27 restricted-role disable
-> spantree cist linkagg 10 restricted-role disable

Release History

Release 7.1.1; command introduced.

Related Commands

spantree mode
Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree vlan restricted-role
Configures the restricted role status for a port or aggregate of ports for the per-VLAN mode VLAN instance.

MIB Objects

vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortRestrictedRole
spantree vlan restricted-role

Configures the restricted role status for a port or a link aggregate of ports for the specified VLAN instance. Enabling this parameter blocks the port from becoming the Root Port, even if it is the most likely candidate for root. Once a Root Port is selected, the restricted port is selected as an Alternate Port.

```
spantree vlan vlan_id {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} {restricted-role | root-guard} {enable | disable}
```

**Syntax Definitions**

- **vlan_id**: An existing VLAN ID number.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **root-guard**: Optional command syntax. Enter `root-guard` instead of restricted-role; both parameters specify the same functionality for this command.
- **enable**: Enables the restricted role status for the specified port-VLAN instance.
- **disable**: Disables the restricted role status for the specified port-VLAN instance.

**Defaults**

By default, the restricted role status for the port is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enabling the restricted role status is used by network administrators to prevent bridges external to the core region of the network from influencing the Spanning Tree topology.
- Note that enabling the restricted role status for a port may impact connectivity within the network.
- This command only applies to the VLAN instance specified by the VLAN ID regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified restricted role status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.
**Examples**

-> spantree vlan 3 linkagg 15 restricted-role enable
-> spantree vlan 3 linkagg 15 root-guard enable
-> spantree vlan 255 port 8/23 restricted-role enable
-> spantree vlan 255 port 8/23 root-guard enable
-> spantree vlan 255 port 8/24-27 restricted-role enable
-> spantree vlan 255 linkagg 11-15 restricted-role enable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**spantree mode**

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

**spantree cist restricted-role**

Configures the restricted role status for a port or aggregate of ports for the flat mode CIST instance.

**MIB Objects**

vStpInsPortTable

  vStpInsPortNumber
  vStpInsPortRestrictedRole
**spantree cist restricted-tcn**

Configures the restricted TCN status for a port or a link aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST). When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

```
spantree cist {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} restricted-tcn {enable | disable}
```

**Syntax Definitions**

- `chassis`  
  The chassis identifier.

- `slot/port[-port2]`  
  The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).

- `agg_id[-agg_id2]`  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- `enable`  
  Enables the restricted TCN status for the specified port-CIST instance.

- `disable`  
  Disables the restricted TCN status for the specified port-CIST instance.

**Defaults**

By default, the restricted TCN status for the port is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enabling the restricted TCN status is used by network administrators to prevent bridges external to the core region of the network from causing unnecessary MAC address flushing in that region.

- Note that enabling the restricted TCN status for a port may impact Spanning Tree connectivity.

- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the per-VLAN mode when this command is used, the specified restricted TCN status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree mode.

**Examples**

- `-> spantree cist linkagg 15 restricted-tcn enable`
- `-> spantree cist port 8/23 restricted-tcn disable`
Distributed Spanning Tree Commands

-> spantree cist port 2/2-4 restricted-tcn enable
-> spantree cist linkagg 10-14 restricted-tcn disable

Release History
Release 7.1.1; command introduced.

Related Commands

spantree mode
Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

spantree vlan restricted-tcn
Configures the restricted TCN status for a port or aggregate of ports for the specified per-VLAN mode VLAN instance.

MIB Objects

vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortRestrictedTcn
**spantree vlan restricted-tcn**

Configures the restricted TCN status for a port or a link aggregate of ports for the specified VLAN instance. When this parameter is enabled, the port does not propagate topology changes and notifications to/from other ports.

```
spantree vlan vlan_id {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} restricted-tcn {enable | disable}
```

**Syntax Definitions**

- `vlan_id`: An existing VLAN ID number.
- `chassis`: The chassis identifier.
- `slot/port[-port2]`: The slot number and port number of the physical port. Use a hyphen to specify a range of ports (4/1-8).
- `agg_id[-agg_id2]`: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `enable`: Enables the restricted TCN status for the specified port-VLAN instance.
- `disable`: Disables the restricted TCN status for the specified port-VLAN instance.

**Defaults**

By default, the restricted TCN is set to disable.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enabling the restricted TCN status is used by network administrators to prevent bridges external to the core region of the network from causing unnecessary MAC address flushing in that region.
- Note that enabling the restricted TCN status for a port may impact Spanning Tree connectivity.
- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.
- If the switch is running in the flat mode when this command is used, the specified restricted TCN status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.
**Examples**

-> spantree vlan 2 linkagg 15 restricted-tcn enable
-> spantree vlan 2 linkagg 16-20 restricted-tcn enable
-> spantree vlan 255 port 8/23 restricted-tcn disable
-> spantree vlan 255 port 8/24-27 restricted-tcn disable

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **spantree mode**
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- **spantree cist restricted-tcn**
  Configures the restricted TCN status for a port or aggregate of ports for the flat mode Common and Internal Spanning Tree (CIST).

**MIB Objects**

vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortRestrictedTcn
**spantree cist txholdcount**

Rate limits the transmission of BPDU through a given port for the flat mode Common and Internal Spanning Tree (CIST) instance.

`spantree cist txholdcount value`

---

**Syntax Definitions**

`value` A numeric value that controls the transmission of BPDU through the port. The valid range is 1–10.

---

**Defaults**

By default, the `txholdcount` value is set to 3.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>availability</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command only applies to the CIST instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the per-VLAN mode when this command is used, the specified `txholdcount` status for the port is not active for the CIST instance until the switch is running in the flat Spanning Tree mode.

---

**Examples**

```plaintext
-> spantree cist txholdcount 5
```

---

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- **spantree mode**
  Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

- **spantree vlan txholdcount**
  Configures the BPDU transmission rate limit for the specified VLAN instance.

**MIB Objects**

- **vStpInsTable**
  - **vStpInsBridgeTxHoldCount**
**spantree vlan txholdcount**

Rate limits the transmission of BPDU through a given port for the VLAN instance.

```
spantree vlan vlan_id txholdcount {value}
```

### Syntax Definitions

- `vlan_id`: An existing VLAN ID number.
- `value`: A numeric value that controls the transmission of BPDU through the port. The valid range is 1–10.

### Defaults

By default, the `txholdcount` value is set to 3.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command only applies to the specified VLAN instance regardless of which operating mode (flat or per-VLAN) is active for the switch.

- If the switch is running in the flat mode when this command is used, the specified `txholdcount` status for the port is not active for the VLAN instance until the switch is running in the per-VLAN Spanning Tree mode.

### Examples

```
-> spantree vlan 3 txholdcount 6
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

**spantree mode**

Selects the Spanning Tree operating mode (flat or per-VLAN) for the switch.

**spantree cist txholdcount**

Configures the BPDU transmission rate limit for the CIST instance.

**MIB Objects**

vStpInsTable

vStpInsBridgeTxHoldCount
show spantree

Displays Spanning Tree bridge information for the flat mode Common and Internal Spanning Tree (CIST) instance or the per-VLAN mode VLAN instances.

Syntax Definitions

N/A

Defaults

NA

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the switch is operating in the per-VLAN mode, this command displays a list of VLAN instances.
- If the switch is operating in the flat mode and the protocol is STP or RSTP, this command displays the single flat mode instance.
- If the switch is operating in the flat mode and the protocol is set to MSTP, this command displays a list of MSTIs, including MSTI 0 (also known as the CIST).

Examples

-> spantree mode flat
-> spantree protocol rstp
-> show spantree

Spanning Tree Path Cost Mode : 32 BIT
Bridge STP Status Protocol Priority(Prio:SysID)
---------------------------------------------
  1   ON  RSTP  32768 (0x8000:0x0000)

output definitions

<table>
<thead>
<tr>
<th>Spanning Tree Path Cost Mode</th>
<th>The Spanning Tree path cost mode for the switch (32 BIT or AUTO) Configured through the <code>spantree path-cost-mode</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge</td>
<td>The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>STP Status</th>
<th>The Spanning Tree state for the CIST instance (ON or OFF).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>The Spanning Tree protocol applied to the instance (STP or RSTP). Configured through the <code>spantree protocol</code> command.</td>
</tr>
<tr>
<td>Priority</td>
<td>The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the <code>spantree priority</code> command.</td>
</tr>
</tbody>
</table>

```plaintext
-> spantree mode flat
-> spantree protocol mstp
```

```plaintext
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
  Msti STP Status Protocol Priority (Prio:SysID)
  +----------------+----------+--------+---------------------+
  0   ON   MSTP   32768 (0x8000:0x0000)
  2   ON   MSTP   32770 (0x8000:0x0002)
  3   ON   MSTP   32771 (0x8000:0x0003)

output definitions

<table>
<thead>
<tr>
<th>Spanning Tree Path Cost Mode</th>
<th>The Spanning Tree path cost mode for the switch (32 BIT or AUTO). Configured through the <code>spantree path-cost-mode</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Msti</td>
<td>The Multiple Spanning Tree Instance (MSTI) instance number. Configured through the <code>spantree msti</code> command. Note that MSTI 0 also represents the CIST instance that is always present on the switch.</td>
</tr>
<tr>
<td>STP Status</td>
<td>The Spanning Tree state for the MSTI (ON or OFF). Configured through the <code>spantree protocol</code> command.</td>
</tr>
<tr>
<td>Priority</td>
<td>The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the <code>spantree priority</code> command.</td>
</tr>
</tbody>
</table>

```plaintext
-> spantree mode per-vlan
-> show spantree
  Spanning Tree Path Cost Mode : AUTO
  Vlan STP Status Protocol Priority
  +----------------+----------+--------+---------------------+
  1   ON   RSTP   32768 (0x8000)
  200  ON   RSTP   32768 (0x8000)
  500  OFF  RSTP   32768 (0x8000)
  4094 OFF  RSTP   32768 (0x8000)
```

output definitions

<table>
<thead>
<tr>
<th>Spanning Tree Path Cost Mode</th>
<th>The Spanning Tree path cost mode for the switch (32 BIT or AUTO). Configured through the <code>spantree path-cost-mode</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan</td>
<td>The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the <code>vlan</code> commands</td>
</tr>
<tr>
<td>STP Status</td>
<td>The Spanning Tree state for the instance (ON or OFF). Configured through the <code>spantree vlan admin-state</code> command.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>The Spanning Tree protocol applied to this instance (STP or RSTP). Configured through the <code>spantree protocol</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the <code>spantree priority</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

- `show spantree cist` Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.
- `show spantree msti` Displays the Spanning Tree bridge configuration for an MSTI instance regardless of which mode (per-VLAN or flat) is active on the switch.
- `show spantree vlan` Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch.

MIB Objects

- `vStpInsTable`
  - `vStpInsNumber`
  - `vStpInsProtocolSpecification`
  - `vStpInsMode`
  - `vStpInsPriority`
  - `vStpInsBridgeAddress`
  - `vStpInsDesignatedRoot`
  - `vStpInsRootCost`
  - `vStpInsRootPortNumber`
  - `vStpInsNextBestRootCost`
  - `vStpInsNextBestRootPortNumber`
  - `vStpInsBridgeTxHoldCount`
  - `vStpInsTopChanges`
  - `vStpInsTimeSinceTopologyChange`
  - `vStpInsMaxAge`
  - `vStpInsForwardDelay`
  - `vStpInsHelloTime`
show spantree cist

Displays the Spanning Tree bridge configuration for the flat mode Common and Internal Spanning Tree (CIST) instance.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guideline**

This command displays Spanning Tree bridge information for the flat mode CIST instance regardless of which mode (per-VLAN or flat) is active on the switch. Note that minimal information is displayed when this command is used in the per-VLAN mode, as the CIST is not active in this mode. See the second example below.

**Examples**

```
-> spantree mode flat
-> show spantree cist
Spanning Tree Parameters for Cist
Spanning Tree Status : ON,
Protocol : IEEE Multiple STP,
mode : FLAT (Single STP),
Auto-Vlan-Containment: Enabled ,
Priority : 32768 (0x8000),
Bridge ID : 8000-2c:fa:a2:24:87:51,
CST Designated Root : 8000-00:e0:bf:cf:26:3d,
Cost to CST Root : 2000,
Designated Root : 8000-2c:fa:a2:24:87:51,
Cost to Root Bridge : 0,
Root Port : 1/1/46,
TxHoldCount : 3,
Topology Changes : 10,
Topology age : 00:01:10,
Last TC Rcvd Port : 1/1/46,
Last TC Rcvd Bridge : 8000-00:e0:bf:cf:26:3d,
```
Current Parameters (seconds)
Max Age = 20,
Forward Delay = 15,
Hello Time = 2

Parameters system uses when attempting to become root
System Max Age = 20,
System Forward Delay = 15,
System Hello Time = 2

-> spantree mode per-vlan
-> show spantree cist
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)

INACTIVE Spanning Tree Parameters for Cist
Spanning Tree Status: ON,
Protocol: IEEE Multiple STP,
Priority: 32768 (0x8000),
TxHoldCount: 5,
System Max Age (seconds) = 10,
System Forward Delay (seconds) = 10,
System Hello Time (seconds) = 5

output definitions
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spanning Tree Status</td>
<td>The Spanning Tree state for the instance (ON or OFF).</td>
</tr>
<tr>
<td>Protocol</td>
<td>The Spanning Tree protocol applied to the CIST (STP, RSTP, or MSTP). Configured through the <code>spantree protocol</code> command.</td>
</tr>
<tr>
<td>Mode</td>
<td>The Spanning Tree operating mode for the switch (per-vlan or flat). Configured through the <code>spantree mode</code> command.</td>
</tr>
<tr>
<td>Auto-Vlan-Containment</td>
<td>The auto VLAN containment status for the instance (Enabled or Disabled). AVC prevents a port that has no VLANs mapped to a Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Configured through the <code>spantree auto-vlan-containment</code> command.</td>
</tr>
<tr>
<td>Priority</td>
<td>The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the <code>spantree priority</code> command.</td>
</tr>
<tr>
<td>Bridge ID</td>
<td>The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.</td>
</tr>
<tr>
<td>CST Designated Root</td>
<td>The bridge identifier for the root of the flat mode CIST instance. This field only appears when MSTP is active on the switch.</td>
</tr>
<tr>
<td>Cost to CST Root</td>
<td>The cost of the path to the root of the flat mode CIST instance. This field only appears when MSTP is active on the switch.</td>
</tr>
<tr>
<td>Designated Root</td>
<td>The bridge identifier for the root of the Spanning Tree for this instance.</td>
</tr>
<tr>
<td>Cost to Root Bridge</td>
<td>The cost of the path to the root for this Spanning Tree instance.</td>
</tr>
<tr>
<td>Root Port</td>
<td>The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.</td>
</tr>
<tr>
<td>Tx Hold Count</td>
<td>The count to limit the transmission of BPDU through the port.</td>
</tr>
<tr>
<td>Topology Changes</td>
<td>The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.</td>
</tr>
</tbody>
</table>
### Distributed Spanning Tree Commands

**show spantree cist**

**Release History**

Release 7.1.1; command introduced.
Release 8.4.1; **Topology Change Port** field added.
Release 8.5R4; **Last TC Rcvd Bridge** field added.

**Related Commands**

- **show spantree**
  - Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.

- **show spantree msti**
  - Displays the Spanning Tree bridge configuration for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.

- **show spantree vlan**
  - Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch.

---

<table>
<thead>
<tr>
<th><strong>output definitions (continued)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Topology age</strong></td>
</tr>
<tr>
<td><strong>Last TC Rcvd Port</strong></td>
</tr>
<tr>
<td><strong>Last TC Rcvd Bridge</strong></td>
</tr>
<tr>
<td><strong>Max Age</strong></td>
</tr>
<tr>
<td><strong>Forward Delay</strong></td>
</tr>
<tr>
<td><strong>Hello Time</strong></td>
</tr>
<tr>
<td><strong>System Max Age</strong></td>
</tr>
<tr>
<td><strong>System Forward Delay</strong></td>
</tr>
<tr>
<td><strong>System Hello Time</strong></td>
</tr>
<tr>
<td><strong>BPDU Switching Enabled</strong></td>
</tr>
</tbody>
</table>
**MIB Objects**

vStpInsTable
  vStpInsNumber
  vStpInsMode
  vStpInsProtocolSpecification
  vStpInsPriority
  vStpInsBridgeAddress
  vStpInsTimeSinceTopologyChange
  vStpInsTopChanges
  vStpInsDesignatedRoot
  vStpInsRootCost
  vStpInsRootPortNumber
  vStpInsNextBestRootPortNumber
  vStpInsNextBestRootCost
  vStpInsMaxAge
  vStpInsHelloTime
  vStpInsBridgeTxHoldCount
  vStpInsForwardDelay
  vStpInsBridgeMaxAge
  vStpInsBridgeHelloTime
  vStpInsBridgeForwardDelay
  vStpInsCistRegionalRootId
  vStpInsCistPathCost
**show spantree msti**

Displays Spanning Tree bridge information for a Multiple Spanning Tree Instance (MSTI).

`show spantree msti [msti_id]`

### Syntax Definitions

**msti_id**

An existing MSTI ID number.

### Defaults

By default, displays information for all MSTIs.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If an **msti_id** number is not specified, this command displays the Spanning Tree status, protocol, and priority values for all MSTIs.
- This command displays Spanning Tree bridge information for an MSTI regardless of which mode (per-VLAN or flat) is active for the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as MSTIs are not active in this mode. In addition, this command fails if MSTP is not the selected flat mode protocol.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the **msti_id** number.

### Examples

```plaintext
-> spantree mode flat
-> spantree protocol mstp
-> show spantree msti
  Spanning Tree Path Cost Mode: AUTO
  Msti STP Status Protocol Priority (Prio:SysID)
  ------------------------------
  0    ON    MSTP    32768 (0x8000:0x0000)
  1    ON    MSTP    32769 (0x8000:0x0001)
-> show spantree msti 0
  Spanning Tree Parameters for Cist
  Spanning Tree Status: ON,
```
Protocol             :   IEEE Multiple STP,
mode                 :   FLAT (Single STP),
Auto-Vlan-Containment:           Enabled   ,
Priority             :        8192 (0x2000),
Bridge ID            :   2000-e8:e7:32:8c:20:09,
CST Designated Root  :   2000-e8:e7:32:8c:20:09,
Cost to CST Root     :                    0,
Designated Root      :   2000-e8:e7:32:8c:20:09,
Cost to Root Bridge  :                    0,
Root Port            :                 None,
TxHoldCount          :                    3,
Topology Changes     :                  203,
Topology age         :             00:00:48,
Last TC Rcvd Port    :                2/1/2,
Last TC Rcvd Bridge  :   3000-e8:e7:32:b9:24:13,
Current Parameters (seconds)
    Max Age              =    20,
    Forward Delay        =    15,
    Hello Time           =     2
Parameters system uses when attempting to become root
    System Max Age       =    20,
    System Forward Delay =    15,
    System Hello Time    =       2

-> spantree mode per-vlan
-> show spantree msti
    Spanning Tree Path Cost Mode : AUTO
** Inactive flat mode instances: **
Msti STP Status Protocol Priority (Prio:SysID)
-----+----------+--------+---------------------
  0      ON      MSTP   32768 (0x8000:0x0000)
  1      ON      MSTP   32769 (0x8000:0x0001)

-> show spantree msti 0
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters for Cist
    Spanning Tree Status : ON,
    Protocol             :   IEEE Multiple STP,
    Priority             :    32768 (0x8000),
    TxHoldCount          :                 3,
    System Max Age (seconds) =    20,
    System Forward Delay (seconds) =    15,
    System Hello Time (seconds) =       2

-> show spantree msti 1
Per Vlan Spanning Tree is enforced !! (Per VLAN mode)
INACTIVE Spanning Tree Parameters for Cist 1
    Spanning Tree Status : ON,
    Protocol             :   IEEE Multiple STP,
    Priority             :    32769 (0x8001),
    TxHoldCount          :                 3,
    System Max Age (seconds) =    20,
    System Forward Delay (seconds) =    15,
    System Hello Time (seconds) =       2
### output definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spanning Tree Path Cost Mode</strong></td>
<td>The Spanning Tree path cost mode for the switch (<strong>32 BIT</strong> or <strong>AUTO</strong>) Configured through the <code>spantree path-cost-mode</code> command.</td>
</tr>
<tr>
<td><strong>Msti</strong></td>
<td>The Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the <code>spantree msti</code> command.</td>
</tr>
<tr>
<td><strong>STP Status</strong></td>
<td>The Spanning Tree state for the instance (<strong>ON</strong> or <strong>OFF</strong>).</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>The Spanning Tree protocol applied to the instance (<strong>STP</strong>, <strong>RSTP</strong>, or <strong>MSTP</strong>). This value is not configurable for an MSTI. Configured through the <code>spantree protocol</code> command.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>The Spanning Tree bridge priority for the instance. The lower the number, the higher the priority. Configured through the <code>spantree priority</code> command.</td>
</tr>
<tr>
<td><strong>Spanning Tree Status Mode</strong></td>
<td>The Spanning Tree state for the instance (<strong>ON</strong> or <strong>OFF</strong>).</td>
</tr>
<tr>
<td><strong>Auto-Vlan-Containment</strong></td>
<td>The auto VLAN containment status for the instance (<strong>Enabled</strong> or <strong>Disabled</strong>). AVC prevents a port that has no VLANs mapped to a Multiple Spanning Tree Instance (MSTI) from becoming the root port for that instance. Configured through the <code>spantree auto-vlan-containment</code> command.</td>
</tr>
<tr>
<td><strong>Bridge ID</strong></td>
<td>The bridge identifier for this Spanning Tree instance. Consists of the bridge priority value (in hex) concatenated with the dedicated bridge MAC address.</td>
</tr>
<tr>
<td><strong>CST Designated Root</strong></td>
<td>The bridge identifier for the root of the flat mode CIST instance. This field only appears when MSTP is active on the switch.</td>
</tr>
<tr>
<td><strong>Cost to CST Root</strong></td>
<td>The cost of the path to the root for the flat mode CIST instance. This field only appears when MSTP is active on the switch.</td>
</tr>
<tr>
<td><strong>Designated Root</strong></td>
<td>The bridge identifier for the root of the Spanning Tree for this instance.</td>
</tr>
<tr>
<td><strong>Cost to Root Bridge</strong></td>
<td>The cost of the path to the root for this Spanning Tree instance.</td>
</tr>
<tr>
<td><strong>Root Port</strong></td>
<td>The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.</td>
</tr>
<tr>
<td><strong>TxHoldCount</strong></td>
<td>The count to limit the transmission of BPDU through the port.</td>
</tr>
<tr>
<td><strong>Topology Changes</strong></td>
<td>The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.</td>
</tr>
<tr>
<td><strong>Topology age</strong></td>
<td>The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (<strong>hh:mm:ss</strong> or <strong>dd days and hh:mm:ss</strong>).</td>
</tr>
<tr>
<td><strong>Last TC Rcvd Port</strong></td>
<td>The port that received the TC Flag Set in RSTP or MSTP protocol BPDU. Default value is None.</td>
</tr>
<tr>
<td><strong>Last TC Rcvd Bridge</strong></td>
<td>The adjacent designated bridge ID received from TC Flag Set in RSTP or MSTP BPDU along with Last TC Rcvd Port. This information is provided only for active RSTP and MSTP topologies. Default value is None.</td>
</tr>
<tr>
<td><strong>Max Age</strong></td>
<td>The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. MSTIs inherit this value from the CIST instance.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Forward Delay</strong></td>
<td>The amount of time (in seconds) that a port remains in the Listening state</td>
</tr>
<tr>
<td></td>
<td>and then the Learning state until it reaches the forwarding state. This</td>
</tr>
<tr>
<td></td>
<td>is also the amount of time used to age out all dynamic entries in the</td>
</tr>
<tr>
<td></td>
<td>Forwarding Database when a topology change occurs. MSTIs inherit this</td>
</tr>
<tr>
<td></td>
<td>value from the CIST instance.</td>
</tr>
<tr>
<td><strong>Hello Time</strong></td>
<td>The amount of time (in seconds) between the transmission of Configuration</td>
</tr>
<tr>
<td></td>
<td>BPDUs on any port that is the Spanning Tree root or is attempting to</td>
</tr>
<tr>
<td></td>
<td>become the Spanning Tree root. MSTIs inherit this value from the CIST</td>
</tr>
<tr>
<td></td>
<td>instance.</td>
</tr>
<tr>
<td><strong>System Max Age</strong></td>
<td>The Max Age value for the root bridge.</td>
</tr>
<tr>
<td><strong>System Forward Delay</strong></td>
<td>The Forward Delay value for the root bridge.</td>
</tr>
<tr>
<td><strong>System Hello Time</strong></td>
<td>The Hello Time value for the root bridge.</td>
</tr>
<tr>
<td><strong>BPDU Switching Enabled</strong></td>
<td>The status of BPDU switching for the instance. This field only appears</td>
</tr>
<tr>
<td></td>
<td>when BPDU switching is enabled. Configured through the **spantree bpdu-</td>
</tr>
<tr>
<td></td>
<td>switching** command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 8.4.1; **Topology Change Port** field added.
Release 8.5R4; **Last TC Rcvd Bridge** field added.

**Related Commands**

- **show spantree**
  Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.

- **show spantree cist**
  Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.

- **show spantree vlan**
  Displays the Spanning Tree bridge configuration for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch.
**MIB Objects**

vStpInsTable
  vStpInsNumber
  vStpInsMode
  vStpInsProtocolSpecification
  vStpInsPriority
  vStpInsBridgeAddress
  vStpInsTimeSinceTopologyChange
  vStpInsTopChanges
  vStpInsDesignatedRoot
  vStpInsRootCost
  vStpInsRootPortNumber
  vStpInsNextBestRootCost
  vStpInsNextBestRootPortNumber
  vStpInsMaxAge
  vStpInsHelloTime
  vStpInsBridgeTxHoldCount
  vStpInsForwardDelay
  vStpInsBridgeMaxAge
  vStpInsBridgeHelloTime
  vStpInsBridgeForwardDelay
  vStpInsCistRegionalRootId
  vStpInsCistPathCost
  vStpInsMstiNumber
**show spantree vlan**

Displays Spanning Tree bridge information for a per-VLAN mode VLAN instance.

**show spantree vlan [vlan_id]**

---

**Syntax Definitions**

*vlan_id*  
An existing VLAN ID number.

---

**Defaults**

By default, displays information for all VLAN instances.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- If a *vlan_id* number is *not* specified, this command displays the Spanning Tree status, protocol, and priority values for all VLAN instances.
- Specify a *vlan_id* number with this command to display Spanning Tree bridge information for a specific VLAN instance.
- This command displays Spanning Tree bridge information for a VLAN instance regardless of which mode (per-VLAN or flat) is active on the switch. Note that minimal information is displayed when this command is used in the flat mode, as VLAN instances are not active in this mode.

---

**Examples**

```
-> spantree mode per-vlan
-> show spantree vlan
  Spanning Tree Path Cost Mode : AUTO
  Vlan STP Status Protocol Priority
  +-------------------------------------------+
  |   vlan   STP  Status  Protocol   Priority |
  +-------------------------------------------+
  |  1   ON    RSTP   32768 (0x8000)          |
  |  200 ON    RSTP   32768 (0x8000)          |
  |  500 OFF   RSTP   32768 (0x8000)          |
  |  4094 OFF  RSTP   32768 (0x8000)          |
  +-------------------------------------------+

-> show spantree vlan 200
  Spanning Tree Parameters for Vlan 200
  Spanning Tree Status : ON,
  Protocol : IEEE Rapid STP,
  mode : Per VLAN (1 STP per Vlan),
```
Distributed Spanning Tree Commands

Priority: 100 (0x0064),
Bridge ID: 0064-e8:e7:32:8c:20:09,
Designated Root: 0064-e8:e7:32:8c:20:09,
Cost to Root Bridge: 0,
Root Port: None,
TxHoldCount: 3,
Topology Changes: 6,
Topology age: 00:00:04,
Last TC Rcvd Port: 2/1/2,
Last TC Rcvd Bridge: 012C-e8:e7:32:b9:24:13,
  Current Parameters (seconds)
    Max Age = 20,
    Forward Delay = 15,
    Hello Time = 2
  Parameters system uses when attempting to become root
    System Max Age = 20,
    System Forward Delay = 15,
    System Hello Time = 2

-> spantree mode flat
-> show spantree vlan 200
Single/Multiple Spanning Tree is enforced !! (flat mode)

INACTIVE Spanning Tree Parameters for Vlan 200
  Spanning Tree Status: ON,
  Protocol: IEEE Rapid STP,
  Priority: 32768 (0x8000),
  TxHoldCount: 3,
  System Max Age (seconds) = 20,
  System Forward Delay (seconds) = 15,
  System Hello Time (seconds) = 2

output definitions

Spanning Tree Path Cost
Mode
  The Spanning Tree path cost mode for the switch (32 BIT or AUTO)
  Configured through the spantree path-cost-mode command.

Vlan
  The VLAN ID associated with the VLAN Spanning Tree instance.
  Configured through the vlan commands

STP Status
  The Spanning Tree state for the instance (ON or OFF).

Protocol
  The Spanning Tree protocol applied to the VLAN instance (STP or
  RSTP). Note that MSTP is not supported for a VLAN instance.
  Configured through the spantree protocol command.

Priority
  The Spanning Tree bridge priority for the instance. The lower the
  number, the higher the priority. Configured through the spantree
  priority command.

Spanning Tree Status
  The Spanning Tree state for the instance (ON or OFF).

Mode
  The Spanning Tree operating mode for the switch (per-vlan or flat).
  Configured through the spantree mode command.

Bridge ID
  The bridge identifier for this Spanning Tree instance. Consists of the
  bridge priority value (in hex) concatenated with the dedicated bridge
  MAC address.

Designated Root
  The bridge identifier for the root of the Spanning Tree for this instance.

Cost to Root Bridge
  The cost of the path to the root for this Spanning Tree instance.
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Root Port</strong></td>
<td>The port that offers the lowest cost path from this bridge to the root bridge for this Spanning Tree instance.</td>
</tr>
<tr>
<td><strong>Tx Hold Count</strong></td>
<td>The count to limit the transmission of BPDU through the port.</td>
</tr>
<tr>
<td><strong>Topology Changes</strong></td>
<td>The number of topology changes detected by this Spanning Tree instance since the management entity was last reset or initialized.</td>
</tr>
<tr>
<td><strong>Topology age</strong></td>
<td>The amount of time (in hundredths of seconds) since the last topology change was detected by this Spanning Tree instance (hh:mm:ss or dd days and hh:mm:ss).</td>
</tr>
<tr>
<td><strong>Last TC Rcvd Port</strong></td>
<td>The port that received the TC Flag Set in RSTP or MSTP protocol BPDU. Default value is None.</td>
</tr>
<tr>
<td><strong>Last TC Rcvd Bridge</strong></td>
<td>The adjacent designated bridge ID received from TC Flag Set in RSTP or MSTP BPDU along with Last TC Rcvd Port. This information is provided only for active RSTP and MSTP topologies. Default value is None.</td>
</tr>
<tr>
<td><strong>Max Age</strong></td>
<td>The amount of time (in seconds) that Spanning Tree Protocol information is retained before it is discarded. Configured through the <code>spantree max-age</code> command.</td>
</tr>
<tr>
<td><strong>Forward Delay</strong></td>
<td>The amount of time (in seconds) that a port remains in the Listening state and then the Learning state until it reaches the forwarding state. This is also the amount of time used to age out all dynamic entries in the Forwarding Database when a topology change occurs. Configured through the <code>spantree forward-delay</code> command.</td>
</tr>
<tr>
<td><strong>Hello Time</strong></td>
<td>The amount of time (in seconds) between the transmission of Configuration BPDU on any port that is the Spanning Tree root or is attempting to become the Spanning Tree root. Configured through the <code>spantree hello-time</code> command.</td>
</tr>
<tr>
<td><strong>System Max Age</strong></td>
<td>The Max Age value for the root bridge.</td>
</tr>
<tr>
<td><strong>System Forward Delay</strong></td>
<td>The Forward Delay value for the root bridge.</td>
</tr>
<tr>
<td><strong>System Hello Time</strong></td>
<td>The Hello Time value for the root bridge.</td>
</tr>
<tr>
<td><strong>BPDU Switching Enabled</strong></td>
<td>The status of BPDU switching for the instance. This field only appears when BPDU switching is enabled. Configured through the <code>spantree bpdu-switching</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 8.4.1; **Topology Change Port** field added.
Release 8.5R4; **Last TC Rcvd Bridge** field added.
Related Commands

**show spantree**
Displays the Spanning Tree bridge configuration for the flat mode CIST instance or a per-VLAN mode VLAN instance, depending on which mode is active for the switch.

**show spantree cist**
Displays the Spanning Tree bridge configuration for the CIST instance regardless of which mode (per-VLAN or flat) is active on the switch.

**show spantree msti**
Displays the Spanning Tree bridge information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.

MIB Objects

`vStpInsTable`  
`vStpInsNumber`  
`vStpInsMode`  
`vStpInsProtocolSpecification`  
`vStpInsPriority`  
`vStpInsBridgeAddress`  
`vStpInsTimeSinceTopologyChange`  
`vStpInsTopChanges`  
`vStpInsDesignatedRoot`  
`vStpInsRootCost`  
`vStpInsRootPortNumber`  
`vStpInsNextBestRootCost`  
`vStpInsNextBestRootPortNumber`  
`vStpInsMaxAge`  
`vStpInsHelloTime`  
`vStpInsBridgeTxHoldCount`  
`vStpInsForwardDelay`  
`vStpInsBridgeMaxAge`  
`vStpInsBridgeHelloTime`  
`vStpInsBridgeForwardDelay`
show spantree ports

Displays Spanning Tree port information.

show spantree ports [forwarding | blocking | active | configured]

Syntax Definitions

forwarding Displays Spanning Tree operational port parameters for ports that are forwarding for the specified instance.

blocking Displays Spanning Tree operational port parameters for ports that are blocked for the specified instance.

active Displays a list of active ports associated with the specified instance.

configured Displays Spanning Tree administrative port parameters for all ports associated with the specified instance.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>forwarding</td>
<td>all ports</td>
</tr>
<tr>
<td>blocking</td>
<td></td>
</tr>
<tr>
<td>active</td>
<td></td>
</tr>
<tr>
<td>configured</td>
<td></td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the switch is operating in the per-VLAN mode, this command displays port information for the VLAN instances.
- If the switch is operating in the flat mode and the protocol is STP or RSTP, this command displays port information for the single flat mode instance.
- If the switch is operating in the flat mode and the protocol is set to MSTP, this command displays port information for the MSTIs, including MSTI 0 (also known as the CIST).

Examples

-> spantree mode flat
-> spantree protocol rstp
-> show spantree ports

<table>
<thead>
<tr>
<th>Bridge</th>
<th>Port</th>
<th>Oper Status</th>
<th>Path Cost</th>
<th>Role</th>
<th>loop-guard</th>
<th>Note</th>
</tr>
</thead>
</table>
Distributed Spanning Tree Commands

show spantree ports

-> spantree protocol mstp
-> show spantree ports

<table>
<thead>
<tr>
<th>Msti</th>
<th>Port</th>
<th>Oper Status</th>
<th>Path Cost</th>
<th>Role</th>
<th>loop-guard</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/3</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/4</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/6</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/7</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/9</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/10</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0/1</td>
<td>BLK</td>
<td>0</td>
<td>ALT</td>
<td>ENA</td>
<td>ERR</td>
</tr>
<tr>
<td>10</td>
<td>1/1</td>
<td>FORW</td>
<td>19</td>
<td>DESG</td>
<td>ENA</td>
<td></td>
</tr>
</tbody>
</table>

-> spantree mode per-vlan
-> show spantree ports

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Port</th>
<th>Oper Status</th>
<th>Path Cost</th>
<th>Role</th>
<th>loop-guard</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1/1</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/1/1</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/2</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/3</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/4</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/5</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1/6</td>
<td>DIS</td>
<td>0</td>
<td>DIS</td>
<td>DIS</td>
<td></td>
</tr>
</tbody>
</table>

-> show spantree ports active

<table>
<thead>
<tr>
<th>Bridge</th>
<th>Port</th>
<th>Oper Status</th>
<th>Path Cost</th>
<th>Role</th>
<th>loop-guard</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>2/1</td>
<td>FORW</td>
<td>19</td>
<td>DESG</td>
<td>ENA</td>
<td></td>
</tr>
<tr>
<td>172</td>
<td>2/8</td>
<td>FORW</td>
<td>19</td>
<td>ROOT</td>
<td>DIS</td>
<td></td>
</tr>
<tr>
<td>1001</td>
<td>2/1</td>
<td>FORW</td>
<td>19</td>
<td>DESG</td>
<td>DIS</td>
<td></td>
</tr>
</tbody>
</table>

-> show spantree ports blocking

<table>
<thead>
<tr>
<th>Bridge</th>
<th>Port</th>
<th>Oper Status</th>
<th>Path Cost</th>
<th>Role</th>
<th>loop-guard</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0/1</td>
<td>BLK</td>
<td>19</td>
<td>DESG</td>
<td>ENA</td>
<td>ERR</td>
</tr>
<tr>
<td>172</td>
<td>2/8</td>
<td>BLK</td>
<td>29</td>
<td>ALT</td>
<td>DIS</td>
<td></td>
</tr>
</tbody>
</table>

output definitions

**Bridge, Msti, or Vlan**

The CIST instance, referred to as bridge 1 when either STP (802.1D) or RSTP (802.1W) is the active protocol in the flat mode. The MSTI number when MSTP is the active protocol in the flat mode. The VLAN ID number when STP or RSTP is the active protocol in the per-VLAN mode.

**Port**

The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
**Output Definitions (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Oper Status</strong></td>
<td>The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, learning, and forwarding.</td>
</tr>
<tr>
<td><strong>Path Cost</strong></td>
<td>The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the <code>spantree msti path-cost</code> or <code>spantree vlan path-cost</code> command.</td>
</tr>
<tr>
<td><strong>Role</strong></td>
<td>The role of the port for this Spanning Tree instance. Possible port roles are: root, designated, alternate, and backup.</td>
</tr>
<tr>
<td><strong>loop-guard</strong></td>
<td>Displays if the loop-guard is enabled (ENA) or disabled (DIS) on the port. Configured through the <code>spantree loop-guard</code> command.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Displays a note if the port has entered the error violation state (ERR); then the port role of the port instance in that row becomes insignificant.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show spantree cist ports` Displays Spanning Tree port information for the flat mode CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
- `show spantree msti ports` Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.
- `show spantree vlan ports` Displays Spanning Tree port information for VLAN instances when the switch is operating in the per-VLAN or flat Spanning Tree mode.
MIB Objects

vStpInsPortTable
  vStpInsPortNumber
  vStpInsPortPriority
  vStpInsPortEnable
  vStpInsPortState
  vStpInsPortManualMode
  vStpInsPortPathCost
  vStpInsPortDesignatedCost
  vStpInsPortRole
  vStpInsPortAdminConnectionType
  vStpInsPortOperConnectionType
  vStpInsPortAdminEdge
  vStpInsPortAutoEdge
  vStpInsPortRestrictedRole
  vStpInsPortRestrictedTcn
  vStpInsPortPrimaryPortNumber
  vStpInsPortDesignatedRoot
  vStpInsPortDesignatedBridge
  vStpPortConfigPVST
  vStpPortConfigStatePVST
  vStpBridgeModePVST
show spantree cist ports

Displays Spanning Tree port information for the flat mode Common and Internal Spanning Tree (CIST) instance.

show spantree cist ports [forwarding | blocking | active | configured]

Syntax Definitions

forwarding Displays Spanning Tree operational port parameters for ports that are forwarding for the CIST instance.

blocking Displays Spanning Tree operational port parameters for ports that are blocked for the CIST instance.

active Displays a list of active ports associated with the CIST instance.

configured Displays Spanning Tree administrative port parameters for the CIST instance.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>forwarding</td>
<td>blocking</td>
</tr>
<tr>
<td>all ports</td>
<td></td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command displays Spanning Tree port information for the flat mode CIST instance regardless of which mode (per-VLAN or flat) is active for the switch.
- Note that minimal information is displayed when this command is used in the per-VLAN mode, as the CIST is not active in this mode.

Examples

-> show spantree cist ports

Spanning Tree Port Summary for Cist

<table>
<thead>
<tr>
<th>Port</th>
<th>Oper</th>
<th>Path</th>
<th>Desig</th>
<th>Prim. Op</th>
<th>Op</th>
<th>Cost</th>
<th>Cost</th>
<th>Role</th>
<th>Port</th>
<th>Cnx</th>
<th>Edg</th>
<th>Desig Bridge ID</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>FORW</td>
<td>200000</td>
<td>52</td>
<td>ROOT</td>
<td>1/1</td>
<td>PTP</td>
<td>EDG</td>
<td>8000-00:30:f1:5b:37:73</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Distributed Spanning Tree Commands

```
1/2  DIS  0  0  DIS 1/2  NS  No  0000-00:00:00:00:00:00
1/3  DIS  0  0  DIS 1/3  NS  EDG  0000-00:00:00:00:00:00
1/4  DIS  0  0  DIS 1/4  NS  No  0000-00:00:00:00:00:00
1/5  DIS  0  0  DIS 1/5  NS  EDG  0000-00:00:00:00:00:00
1/6  DIS  0  0  DIS 1/6  NS  EDG  0000-00:00:00:00:00:00
1/7  DIS  0  0  DIS 1/7  NS  EDG  0000-00:00:00:00:00:00
1/8  DIS  0  0  DIS 1/8  NS  No  0000-00:00:00:00:00:00
```

-> show spantree cist ports active

Spanning Tree Port Summary for Cist

```
<table>
<thead>
<tr>
<th>Oper St</th>
<th>Path Cost</th>
<th>Desig Cost</th>
<th>Role</th>
<th>Prim. Op</th>
<th>Op Cnx Edg</th>
<th>Bridge ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/1</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/2</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/3</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/4</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/5</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
</tbody>
</table>
```

-> show spantree cist ports

Per Vlan Spanning Tree is enforced !! (Per VLAN mode)

INACTIVE Spanning Tree Parameters

```
<table>
<thead>
<tr>
<th>Oper St</th>
<th>Path Cost</th>
<th>Desig Cost</th>
<th>Role</th>
<th>Prim. Op</th>
<th>Op Cnx Edg</th>
<th>Bridge ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/1</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/2</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/3</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/4</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
<tr>
<td>DIS</td>
<td>0</td>
<td>0</td>
<td>DIS 1/5</td>
<td>NS</td>
<td>0000-00:00:00:00:00:00</td>
<td></td>
</tr>
</tbody>
</table>
```

output definitions

- **Port**: The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).
- **Oper St**: The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.
- **Path Cost**: The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the `spantree vlan path-cost` command.
- **Desig Cost**: The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.
- **Role**: The role of the port for this Spanning Tree instance. Possible port roles are: **root**, **designated**, **alternate**, and **backup**.
- **Prim. Port**: The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
- **Op Cnx**: Operational connection type: **PTP**, **NPT**, or **NS** (nonsignificant). Shows the current operational state of the port connection type. See the `spantree vlan connection` command for more information.
-- show spantree cist ports configured

Spanning Tree Port Admin Configuration for Vlan 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>St. Mode</th>
<th>Cost</th>
<th>Cnx</th>
<th>Edg</th>
<th>Edg Tcn</th>
<th>Root Guard</th>
<th>Cfg Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>No</td>
<td>AUT Off</td>
</tr>
<tr>
<td>1/2</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>0</td>
<td>NPT</td>
<td>No</td>
<td>Yes</td>
<td>AUT Off</td>
</tr>
<tr>
<td>1/3</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>0</td>
<td>NPT</td>
<td>No</td>
<td>Yes</td>
<td>AUT Off</td>
</tr>
<tr>
<td>1/4</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>0</td>
<td>NPT</td>
<td>No</td>
<td>Yes</td>
<td>AUT Off</td>
</tr>
<tr>
<td>1/5</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>0</td>
<td>NPT</td>
<td>No</td>
<td>Yes</td>
<td>AUT Off</td>
</tr>
</tbody>
</table>

output definitions (continued)

- **Op Edg**: Operational connection type: **EDG**. Shows the current operational state of the port connection type. See the `spantree vlan connection` command for more information.

- **Desig Bridge ID**: The bridge identifier for the designated bridge for this port segment.

output definitions

- **Port**: The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).

- **Port Pri**: The Spanning Tree priority for the port. The lower the number, the higher the priority.

- **Adm St**: The Spanning Tree administrative status of the port: **enabled** or **disabled**.

- **Man. Mode**: The manual mode setting for the port: **yes** indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; **no** indicates that the Spanning Tree Algorithm is managing the port state. Configured through the `spantree vlan path-cost` command.

- **Config Cost**: The configured path cost value for this port. Configured through the `spantree vlan path-cost` command.

- **Adm Cnx**: The administrative connection type: **PTP**, **NPT**, or **AUT**. Configured through the `spantree vlan connection` command.

- **Adm Edg**: The edge port administrative status: **yes** indicates that the port is an admin edge port; **no** indicates that the port is not an admin edge port. Configured through the `spantree vlan connection` command.

- **Aut Edg**: The edge port automatic status: **yes** indicates that the port is an automatic edge port; **no** indicates that the port is not an automatic edge port. Configured through the `spantree cist auto-edge` or `spantree vlan auto-edge` command.
**output definitions (continued)**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rstr Tcn</strong></td>
<td>The restricted TCN capability: <strong>yes</strong> indicates that the port supports the restricted TCN capability; <strong>no</strong> indicates that the port does not support the restricted TCN capability. Configured through the <code>spantree cist restricted-tcn</code> or <code>spantree vlan restricted-tcn</code> command.</td>
</tr>
<tr>
<td><strong>Rstr Role</strong></td>
<td>The restricted role port status: <strong>yes</strong> indicates that the port is a restricted role port; <strong>no</strong> indicates that the port is not a restricted role port. Configured through the <code>spantree cist restricted-role</code> or <code>spantree vlan restricted-role</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **show spantree ports**
  Implicit command for displaying Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.

- **show spantree msti ports**
  Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.

**MIB Objects**

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortPriority`
  - `vStpInsPortState`
  - `vStpInsPortEnable`
  - `vStpInsPortPathCost`
  - `vStpInsPortDesignatedCost`
  - `vStpInsPortDesignatedBridge`
  - `vStpInsPortAdminEdge`
  - `vStpInsPortAutoEdge`
  - `vStpInsPortRestrictedRole`
  - `vStpInsPortRestrictedTcn`
  - `vStpInsPortManualMode`
  - `vStpInsPortRole`
  - `vStpInsPrimaryPortNumber`
  - `vStpInsPortAdminConnectionType`
  - `vStpInsPortOperConnectionType`
**show spantree msti ports**

Displays Spanning Tree port information for a flat mode Multiple Spanning Tree Instance (MSTI).

`show spantree msti [msti_id] ports [forwarding | blocking | active | configured]`

---

### Syntax Definitions

- **msti_id**
  - An existing MSTI ID number.

- **forwarding**
  - Displays Spanning Tree operational port parameters for ports that are forwarding for the MSTI instance.

- **blocking**
  - Displays Spanning Tree operational port parameters for ports that are blocked for the MSTI instance.

- **active**
  - Displays a list of active ports associated with the MSTI instance.

- **configured**
  - Displays Spanning Tree administrative port parameters for the MSTI instance.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>msti_id</td>
<td>all MSTIs</td>
</tr>
<tr>
<td>forwarding</td>
<td>all ports</td>
</tr>
<tr>
<td>blocking</td>
<td>all ports</td>
</tr>
<tr>
<td>active</td>
<td>all ports</td>
</tr>
<tr>
<td>configured</td>
<td>all ports</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- If an `msti_id` number is not specified, this command displays the Spanning Tree port operational status, path cost, and role values for all associated MSTIs.

- This command displays Spanning Tree port information for an MSTI regardless of which mode (per-VLAN or flat) is active on the switch.

- Note that minimal information is displayed when this command is used in the per-VLAN mode, as MSTIs are not active in this mode. In addition, if MSTP is not the selected flat mode protocol, this command fails.

- The `configured` keyword is only available when an instance number is specified with this command. In addition, this keyword cannot be used in combination with either the `forwarding` or `blocking` keywords.
- Note that MSTI 0 also represents the CIST instance that is always present on the switch. To view the CIST instance using this command, specify zero (0) for the `msti_id` number.

## Examples

```
-> show spantree msti ports
Msti  Port  Oper Status  Path Cost  Role
-----+-----+------------+---------+-----
  0  1/1  FORW       200000   ROOT
  0  1/2  DIS           0    DIS
  0  1/3  DIS           0    DIS
  0  1/4  DIS           0    DIS
  0  1/5  DIS           0    DIS
  0  1/6  DIS           0    DIS
  0  1/7  DIS           0    DIS
  0  1/8  DIS           0    DIS
  0  1/9  DIS           0    DIS
  0  1/10 DIS           0    DIS
  0  1/11 DIS           0    DIS
  0  1/12 DIS           0    DIS
  0  1/13 DIS           0    DIS
  0  1/14 DIS           0    DIS
  0  1/15 DIS           0    DIS
  0  1/16 DIS           0    DIS
  0  1/17 DIS           0    DIS
  0  1/18 DIS           0    DIS
  0  1/19 DIS           0    DIS
  0  1/20 DIS           0    DIS
  0  1/21 DIS           0    DIS
  0  1/22 DIS           0    DIS
  0  1/23 DIS           0    DIS
  0  1/24 DIS           0    DIS
  0  5/1 DIS           0    DIS
  0  5/2 DIS           0    DIS
  1  1/1  FORW       200000   MSTR
  1  1/2  DIS           0    DIS
  1  1/3  DIS           0    DIS
  1  1/4  DIS           0    DIS
  1  1/5  DIS           0    DIS
  1  1/6  DIS           0    DIS
  1  1/7  DIS           0    DIS
  1  1/8  DIS           0    DIS
  1  1/9  DIS           0    DIS
  1  1/10 DIS           0    DIS
  1  1/11 DIS           0    DIS
  1  1/12 DIS           0    DIS
  1  1/13 DIS           0    DIS
  1  1/14 DIS           0    DIS
  1  1/15 DIS           0    DIS
  1  1/16 DIS           0    DIS
  1  1/17 DIS           0    DIS
  1  1/18 DIS           0    DIS
  1  1/19 DIS           0    DIS
  1  1/20 DIS           0    DIS
  1  1/21 DIS           0    DIS
  1  1/22 DIS           0    DIS
  1  1/23 DIS           0    DIS
  1  1/24 DIS           0    DIS
```
Distributed Spanning Tree Commands

show spantree msti ports

```
 1 5/1  DIS  0  DIS
 1 5/2  DIS  0  DIS
```

-> show spantree msti 0 ports

Per Vlan Spanning Tree is enforced !! (Per VLAN mode)

INACTIVE Spanning Tree Parameters

<table>
<thead>
<tr>
<th>Port</th>
<th>Oper St</th>
<th>Path Cost</th>
<th>Desig Cost</th>
<th>RSTR Role/ Root Guard</th>
<th>Prim. Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
-> show spantree msti 0 ports configured
```

Spanning Tree Port Admin Configuration for Vlan 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>Adm Man. Config</th>
<th>Adm St. Mode</th>
<th>Cost</th>
<th>Cnx Edg</th>
<th>Edg Tcn</th>
<th>Root Guard</th>
<th>Cfg Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

**Msti**
The Multiple Spanning Tree Instance (MSTI) number. MSTI 0 represents the CIST. Configured through the `spantree msti` command.

**Port**
The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).

**Oper St**
The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.

**Path Cost**
The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the `spantree msti path-cost` command.

**Desig Cost**
The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.

**RSTR Role/ Root Guard**
The role of the port for this Spanning Tree instance. Possible port roles are: root, designated, alternate, master, and backup.

**Prim. Port**
The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.
**output definitions (continued)**

**Op Cnx**
Operational connection type: PTP, NPT, or NS (nonsignificant). Shows the current operational state of the port connection type. See the `spantree vlan connection` command for more information.

**Op Edg**
Operational connection type: EDG. Shows the current operational state of the port connection type. See the `spantree vlan connection` command for more information.

**Desig Bridge ID**
The bridge identifier for the designated bridge for this port segment.

**PVST+ Cfg**
Indicates the current PVST+ port configuration (auto, enable or disable).

**PVST+ Stat**
Indicates the current status of the PVST+ mode (On or Off).

```
-> show spantree msti 2 ports configured
Spanning Tree Port Admin Configuration for Msti 2

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>St. Mode</th>
<th>Cost</th>
<th>Cnx</th>
<th>Edg</th>
<th>Edg</th>
<th>Tcn</th>
<th>Root Guard</th>
<th>Opt.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/2</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/3</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/4</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/5</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/6</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/7</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/8</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/9</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/10</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/11</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
<tr>
<td>1/12</td>
<td>7</td>
<td>ENA</td>
<td>0</td>
<td>AUT</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>DIS</td>
</tr>
</tbody>
</table>
```

**output definitions (continued)**

**Port**
The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (for example, 0/31).

**Port Pri**
The Spanning Tree priority for the port. It is a numeric value and the lower the number, the higher the priority. Configured through the `spantree priority` command.

**Adm St**
The Spanning Tree administrative status of the port: enabled - ENA or disabled - DIS.

**Man. Mode**
The manual mode setting for the port: yes indicates that the blocking or forwarding state of the port was manually set and the port does not participate in the Spanning Tree Algorithm; no indicates that the Spanning Tree Algorithm is managing the port state. Configured through the `spantree vlan path-cost` command.

**Config Cost**
The configured path cost value for this port. Configured through the `spantree msti path-cost` command.

**Adm Cnx**
The administrative connection type: PTP, NPT, or AUT. Configured through the `spantree vlan connection` command.
### Output Definitions (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adm Edg</strong></td>
<td>The edge port administrative status: <strong>yes</strong> indicates that the port is an admin edge port; <strong>no</strong> indicates that the port is not an admin edge port. Configured through the <code>spantree vlan connection</code> command.</td>
</tr>
<tr>
<td><strong>Aut Edg</strong></td>
<td>The edge port automatic status: <strong>yes</strong> indicates that the port is an automatic edge port; <strong>no</strong> indicates that the port is not an automatic edge port. Configured through the <code>spantree cist auto-edge</code> or <code>spantree vlan auto-edge</code> command.</td>
</tr>
<tr>
<td><strong>Rstr Tcn</strong></td>
<td>The restricted TCN capability: <strong>yes</strong> indicates that the port supports the restricted TCN capability; <strong>no</strong> indicates that the port does not support the restricted TCN capability. Configured through the <code>spantree cist restricted-ten</code> or <code>spantree vlan restricted-ten</code> command.</td>
</tr>
<tr>
<td><strong>Rstr Role</strong></td>
<td>The restricted role port status: <strong>yes</strong> indicates that the port is a restricted role port; <strong>no</strong> indicates that the port is not a restricted role port. Configured through the <code>spantree cist restricted-role</code> or <code>spantree vlan restricted-role</code> command.</td>
</tr>
</tbody>
</table>

### Related Commands

- **show spantree ports**  
  Displays Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.
- **show spantree cist ports**  
  Displays Spanning Tree port information for a CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.
- **show spantree vlan ports**  
  Displays Spanning Tree port information for a VLAN when the switch is operating in the per-VLAN or flat Spanning Tree mode.

### MIB Objects

- `vStpInsPortTable`
  - `vStpInsPortNumber`
  - `vStpInsPortPriority`
  - `vStpInsPortState`
  - `vStpInsPortEnable`
  - `vStpInsPortPathCost`
  - `vStpInsPortDesignatedCost`
  - `vStpInsPortDesignatedBridge`
  - `vStpInsPortAdminEdge`
  - `vStpInsPortAutoEdge`
  - `vStpInsPortRestrictedRole`
  - `vStpInsPortRestrictedTcn`
  - `vStpInsPortManualMode`
  - `vStpInsPortRole`
  - `vStpPortConfigPVST`
  - `vStpPortConfigStatePVST`
  - `vStpBridgeModePVST`
  - `vStpInsPrimaryPortNumber`
  - `vStpInsPortAdminConnectionType`
  - `vStpInsPortOperConnectionType`
**show spantree vlan ports**

Displays Spanning Tree port information for a VLAN instance.

**Command Syntax**

```text
show spantree vlan [vlan_id|-vlan_id2] ports [forwarding | blocking | active | configured]
```

**Syntax Definitions**

- **vlan_id|-vlan_id2**: An existing VLAN ID number. Use a hyphen to specify a range of VLAN IDs (for example, `vlan 10-15`).
- **forwarding**: Displays Spanning Tree operational port parameters for ports that are forwarding for the VLAN instance.
- **blocking**: Displays Spanning Tree operational port parameters for ports that are blocked for the VLAN instance.
- **active**: Displays a list of active ports associated with the VLAN instance.
- **configured**: Displays Spanning Tree administrative port parameters for the VLAN instance.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>all VLAN instances</td>
</tr>
<tr>
<td><code>forwarding</code>, <code>blocking</code>, <code>active</code>, <code>configured</code></td>
<td>all ports</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a `vlan_id` number is not specified, this command displays the Spanning Tree port operational status, path cost, and role values for all VLAN instances.

- Specifying a range of VLAN IDs is also allowed. Use a hyphen to indicate a contiguous range (e.g., *show spantree vlan 10-15 ports*). Note that only one VLAN entry—a single VLAN ID or a range of VLAN IDs—is allowed with this command. Multiple entries are not accepted.

- This command displays Spanning Tree port information for a VLAN instance regardless of which mode (per-VLAN or flat) is active for the switch.

- Note that minimal information is displayed when this command is used in the flat mode, as VLAN instances are not active in this mode.
• The **configured** keyword is only available when a VLAN ID is specified with this command. In addition, this keyword cannot be used in combination with either the **forwarding** or **blocking** keywords.

**Examples**

```
-> show spantree vlan ports
Vlan  Port Oper Status  Path Cost  Role    Note
-----+-----+------------+---------+-------+---------
1   1/1       DIS           0    DIS
1   1/2       DIS           0    DIS
1   1/3       DIS           0    DIS
1   1/4       DIS           0    DIS
1   1/5       DIS           0    DIS
1   1/6       DIS           0    DIS
1   1/7       DIS           0    DIS
1   1/8       DIS           0    DIS
1   1/9       DIS           0    DIS
1   1/10      DIS           0    DIS
1   1/11     FORW          19    DIS
1   1/12

-> show spantree vlan 1 ports
Spanning Tree Port Summary for Vlan 1
Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
1/1   DIS       0       0    DIS 1/1   NS EDG 0000-00:00:00:00:00:00
1/2   DIS       0       0    DIS 1/2   NS NO 0000-00:00:00:00:00:00
1/3   DIS       0       0    DIS 1/3   NS NO 0000-00:00:00:00:00:00
1/4   DIS       0       0    DIS 1/4   NS NO 0000-00:00:00:00:00:00
1/5   DIS       0       0    DIS 1/5   NS NO 0000-00:00:00:00:00:00
1/6   DIS       0       0    DIS 1/6   NS NO 0000-00:00:00:00:00:00
1/7   DIS       0       0    DIS 1/7   NS NO 0000-00:00:00:00:00:00
1/8   DIS       0       0    DIS 1/8   NS NO 0000-00:00:00:00:00:00
1/9   DIS       0       0    DIS 1/9   NS NO 0000-00:00:00:00:00:00
1/10  DIS       0       0    DIS 1/10  NS NO 0000-00:00:00:00:00:00
1/11  DIS       0       0    DIS 1/11  NS NO 0000-00:00:00:00:00:00
1/12  FORW      19       0    DIS 1/12 PTP NO 0001-00:d0:95:6a:79:50

-> show spantree vlan 1 ports active
Spanning Tree Port Summary for Vlan 1
Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
1/12  FORW      19       0    DIS 1/12 PTP EDG 0001-00:d0:95:6a:79:50

-> show spantree vlan 10-13 ports
Spanning Tree Port Summary for Vlan 10
Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
1/46  DIS       0       0    DIS 1/46 NS EDG 0000-00:00:00:00:00:00

Spanning Tree Port Summary for Vlan 11
Oper  Path   Desig        Prim. Op  Op
Port   St   Cost    Cost   Role Port  Cnx Edg Desig Bridge ID         Note
-----+----+-------+-------+----+-----+---+---+----------------------+---------
1/36  DIS       0       0    DIS 1/36 NS EDG 0000-00:00:00:00:00:00
1/37  DIS       0       0    DIS 1/37 NS NO 0000-00:00:00:00:00:00
```
Spanning Tree Port Summary for Vlan 12

<table>
<thead>
<tr>
<th>Oper St</th>
<th>Port</th>
<th>Oper</th>
<th>Path Cost</th>
<th>Cost</th>
<th>Role</th>
<th>Prim. Port</th>
<th>Op Cnx</th>
<th>Op Edg</th>
<th>Desig Bridge ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIS</td>
<td>1/42</td>
<td>DIS</td>
<td>1/42</td>
<td>0</td>
<td>NS</td>
<td>1/42</td>
<td>NS</td>
<td>EDG</td>
<td>0000-00:00:00:00:00:00</td>
</tr>
<tr>
<td>DIS</td>
<td>1/43</td>
<td>DIS</td>
<td>1/43</td>
<td>0</td>
<td>NS</td>
<td>1/43</td>
<td>NS</td>
<td>NO</td>
<td>0000-00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

Spanning Tree Port Summary for Vlan 13

<table>
<thead>
<tr>
<th>Oper St</th>
<th>Port</th>
<th>Oper</th>
<th>Path Cost</th>
<th>Cost</th>
<th>Role</th>
<th>Prim. Port</th>
<th>Op Cnx</th>
<th>Op Edg</th>
<th>Desig Bridge ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIS</td>
<td>1/38</td>
<td>DIS</td>
<td>1/38</td>
<td>0</td>
<td>NS</td>
<td>1/38</td>
<td>NS</td>
<td>EDG</td>
<td>0000-00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Vlan</th>
<th>The VLAN ID associated with the VLAN Spanning Tree instance. Configured through the <code>vlan</code> commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).</td>
</tr>
<tr>
<td>Oper St</td>
<td>The port operational state as defined by application of the Spanning Tree Protocol. Possible port operational states include: disabled, blocking, listening, learning, and forwarding.</td>
</tr>
<tr>
<td>Path Cost</td>
<td>The contribution of this port to the path cost towards the Spanning Tree root bridge that includes this port. Path cost is a measure of the distance of the listed port from the root bridge in the number of hops. Configured through the <code>spantree vlan path-cost</code> command.</td>
</tr>
<tr>
<td>Desig Cost</td>
<td>The path cost of the Designated Port of the segment connected to this port. If this is the root bridge or the Spanning Tree status of the port is administratively disabled, this value is 0.</td>
</tr>
<tr>
<td>Role</td>
<td>The role of the port for this Spanning Tree instance. Possible port roles are: root, designated, alternate, master, and backup.</td>
</tr>
<tr>
<td>Prim. Port</td>
<td>The slot number for the module and the physical port number on that module for the primary port associated with this Spanning Tree instance. This information is only available if the port role is backup.</td>
</tr>
<tr>
<td>Op Cnx</td>
<td>Operational connection type: PTP, NPT, or NS (nonsignificant). Shows the current operational state of the port’s connection type. See the <code>spantree vlan connection</code> command for more information.</td>
</tr>
<tr>
<td>Op Edg</td>
<td>Operational connection type: EDG. Shows the current operational state of the port’s connection type. See the <code>spantree vlan connection</code> command for more information.</td>
</tr>
<tr>
<td>Desig Bridge ID</td>
<td>The bridge identifier for the designated bridge for this port’s segment.</td>
</tr>
</tbody>
</table>
show spantree vlan 1 ports configured

Spanning Tree Port Admin Configuration for Vlan 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>St. Mode</th>
<th>Cost</th>
<th>Cnx</th>
<th>Edg Edg Tcn</th>
<th>Root Guard</th>
<th>Cfg Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/2</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/3</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/4</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/5</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/6</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/7</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/8</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/9</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/10</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/11</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/12</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
</tbody>
</table>

show spantree vlan 10-13 ports configured

Spanning Tree Port Admin Configuration for Vlan 10

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>St. Mode</th>
<th>Cost</th>
<th>Cnx</th>
<th>Edg Edg Tcn</th>
<th>Root Guard</th>
<th>Cfg Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/46</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
</tbody>
</table>

Spanning Tree Port Admin Configuration for Vlan 11

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>St. Mode</th>
<th>Cost</th>
<th>Cnx</th>
<th>Edg Edg Tcn</th>
<th>Root Guard</th>
<th>Cfg Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/36</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/37</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
</tbody>
</table>

Spanning Tree Port Admin Configuration for Vlan 12

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>St. Mode</th>
<th>Cost</th>
<th>Cnx</th>
<th>Edg Edg Tcn</th>
<th>Root Guard</th>
<th>Cfg Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/42</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
<tr>
<td>1/43</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
</tbody>
</table>

Spanning Tree Port Admin Configuration for Vlan 13

<table>
<thead>
<tr>
<th>Port</th>
<th>Pri</th>
<th>St. Mode</th>
<th>Cost</th>
<th>Cnx</th>
<th>Edg Edg Tcn</th>
<th>Root Guard</th>
<th>Cfg Stat</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/38</td>
<td>7</td>
<td>ENA</td>
<td>No</td>
<td>No</td>
<td>Yes No No</td>
<td>AUT</td>
<td>OFF</td>
</tr>
</tbody>
</table>

**output definitions**

**Port**

The slot number for the module and the physical port number or a logical port. If the slot number is 0, then the port number refers to a link aggregate logical port number (e.g., 0/31).

**Port Pri**

The Spanning Tree priority for the port (0–15). The lower the number, the higher the priority. Configured through the `spantree priority` command.

**Adm St**

The Spanning Tree administrative status of the port: enabled or disabled. Configured through the `spantree vlan` command to enable or disable Spanning Tree on a port.
### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **show spantree ports**
  Displays Spanning Tree port information for the flat mode CIST instance or a per-VLAN mode VLAN instance.

- **show spantree cist ports**
  Displays Spanning Tree port information for a CIST instance when the switch is operating in the per-VLAN or flat Spanning Tree mode.

- **show spantree msti ports**
  Displays Spanning Tree port information for an MSTI when the switch is operating in the per-VLAN or flat Spanning Tree mode.

**MIB Objects**

- **vStpInsPortTable**
  - **vStpInsPortNumber**
  - **vStpInsPortPriority**
  - **vStpInsPortState**
  - **vStpInsPortEnable**
  - **vStpInsPortPathCost**
  - **vStpInsPortDesignatedCost**
  - **vStpInsPortDesignatedBridge**
  - **vStpInsPortAdminConnectionType**
  - **vStpInsPortOperConnectionType**
  - **vStpInsPortAdminEdge**
  - **vStpInsPortAutoEdge**
  - **vStpInsPortRestrictedRole**
  - **vStpInsPortRestrictedTcn**
  - **vStpInsPortManualMode**
  - **vStpInsPortRole**
  - **vStpInsPrimaryPortNumber**
  - **vStpInsPortAdminConnectionType**
  - **vStpInsPortOperConnectionType**
show spantree mode

Displays the current global Spanning Tree mode parameter values for the switch.

show spantree mode

Syntax Definition

N/A

Defaults

NA

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The global parameters for spanning tree can be activated or configured using the related commands.

Examples

```plaintext
-> show spantree mode
```

Spanning Tree Global Parameters
- Current Running Mode: Per VLAN,
- Current Protocol: N/A (Per VLAN),
- Path Cost Mode: 32 BIT,
- Auto Vlan Containment: N/A
- Cisco PVST+ mode: Disabled
- Vlan Consistency check: Disabled

Output Definitions

- **Current Running Mode**: The spanning tree active on the switch. (Flat or Per VLAN)
- **Current Protocol**: The spanning tree protocol active on the switch.
- **Path Cost Mode**: The path cost mode value configured on the switch. (AUTO or 32 BIT)
- **Auto Vlan Containment**: The Auto VLAN containment mode configured on the switch (Enabled or Disabled).
- **Cisco PVST+ mode**: The PVST+ mode configured on the switch (Enabled or Disabled).
- **Vlan Consistency check**: Specifies if VLAN consistency check is Enabled or Disabled on the switch.
Related Commands

**spantree mode**
Assigns a flat Spanning Tree or per-VLAN Spanning Tree operating mode for the switch.

**spantree protocol**
Configures the Spanning Tree protocol for the flat mode Common and Internal Spanning Tree (CIST) instance or for an individual VLAN instance if the switch is running in the per-VLAN mode.

**spantree path-cost-mode**
Configures the automatic selection of a 16-bit path cost for STP/RSTP ports and a 32-bit path cost for MSTP ports or sets all path costs to use a 32-bit value.

**spantree pvst+compatibility**
Enables or disables PVST+ mode on the switch, port or link aggregate enabling them to operate with Cisco switches.

**spantree auto-vlan-containment**
Enables or disables Auto VLAN Containment (AVC).

Release History
Release 7.1.1; command introduced.

MIB Objects

- vStpTable
  - vStpMode
- vStpInsTable
  - vStpInsProtocolSpecification
- vStpBridge
  - vStpPathCostMode
- vStpMstRegionTable
  - vStpBridgeModePVST
- vStpBridge
  - vStpBridgeAutoVlanContainment
show spantree mst

Displays the Multiple Spanning Tree (MST) information for a MST region or the specified port or link aggregate on the switch.

```
show spantree mst {region | port chassis/slot/port | linkagg agg_id}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number and port number of the physical port.
- **agg_id[-agg_id2]**: The link aggregate ID number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Three MST region attributes (configuration name, revision level, and configuration digest) define an MST region as required by the IEEE 802.1Q 2005 standard. Switches that share the same values for these attributes are all considered part of the same region. Currently each switch can belong to one MST region at a time.

- This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.

- Specify the port number or link aggregate ID along with the **port** or **linkagg** keyword to get information related to the specified port or link aggregate.

### Examples

```
-> show spantree mst region
Configuration Name   = Region 1
Revision Level       = 0
Configuration Digest = 0xac36177f 50283cd4 b83821d8 ab26de62
Revision Max hops    = 20
Cist Instance Number = 0
```
show spantree mst port 1/2

```
MST  Role  State  Pth  Cst  Edge  Boundary  Op  Cnx  Vlans
---+-----+-----+----+--------+--------+-----+-----+--------------
 0  DIS  DIS  0  NO   YES     NS    1
12  DIS  DIS  0  NO    YES     NS
```

show spantree mst linkagg 4

```
MST  Role  State  Pth  Cst  Edge  Boundary  Op  Cnx  Vlans
---+-----+-----+----+--------+--------+-----+-----+--------------
 0  DESG  FORW  6000  NO    NO     NS    1
 1  DESG  FORW  0  NO    NO     NS
 2  DESG  FORW  0  NO    NO     NS
```

**Output Definitions**

- **Configuration Name**: An alphanumeric string that identifies the name of the MST region. Use the `spantree mst region name` command to define this value.
- **Revision Level**: A numeric value that identifies the MST region revision level for the switch.
- **Configuration Digest**: An MST region identifier consisting of a 16 octet hex value (as per the IEEE 802.1Q 2005 standard) that represents all defined MSTIs and their associated VLAN ranges. Use the `spantree msti` and `spantree msti vlan` commands to define VLAN to MSTI associations.
- **Revision Max hops**: The number of maximum hops authorized for region information. Configured through the `spantree mst region max-hops` command.
- **Cist Instance Number**: The number of the CIST instance, which is currently zero as there is only one region per switch. Therefore, only one CIST exists per switch. Note that this instance is also known as the flat mode instance and is known as bridge 1 when using STP or RSTP.

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show spantree msti vlan-map`: Displays the range of VLANs associated to the specified MSTI.
- `show spantree cist vlan-map`: Displays the range of VLANs associated to the CIST instance.
- `show spantree map-msti`: Displays the MSTI that is associated to the specified VLAN.

**MIB Objects**

- `vStpMstRegionTable`
  - `vStpMstRegionNumber`
  - `vStpMstRegionConfigDigest`
  - `vStpMstRegionConfigName`
  - `vStpMstRegionConfigRevisionLevel`
  - `vStpMstRegionCistInstanceNumber`
  - `vStpMstRegionMaxHops`
show spantree msti vlan-map

Displays the range of VLANs associated with the specified Multiple Spanning Tree Instance (MSTI).

show spantree msti [msti_id] vlan-map

Syntax Definitions

msti_id

An existing MSTI ID number.

Defaults

By default, the VLAN to MSTI mapping is displayed for all MSTIs.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- If an msti_id is not specified, then the VLAN to MSTI mapping for all defined MSTIs is displayed.
- This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance.

Examples

-> show spantree msti vlan-map
   Cist
   Name               : 
   VLAN list          : 1-9,14-4094

   Msti 1
   Name               : 
   VLAN list          : 10-11

   Msti 2
   Name               : 
   VLAN list          : 12-13

-> show spantree msti 2 vlan-map
   Msti 2
   Name               : MS1,
   VLAN list          : 12-13
Distributed Spanning Tree Commands

**show spantree msti vlan-map**

### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cist Instance</strong></td>
<td>Identifies MSTI VLAN mapping information for the CIST instance.</td>
</tr>
<tr>
<td><strong>Msti</strong></td>
<td>The MSTI ID number that identifies an association between a Spanning Tree instance and a range of VLANs.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td>An alphanumeric value that identifies an MSTI name. Use the <code>spantree msti</code> command to define an MSTI name.</td>
</tr>
<tr>
<td><strong>VLAN list</strong></td>
<td>The range of VLAN IDs that are associated with this MSTI.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command introduced.

### Related Commands

- `show spantree mst` Displays the MST region information for the switch.
- `show spantree cist vlan-map` Displays the range of VLANs associated to the CIST instance.
- `show spantree map-msti` Displays the MSTI that is associated to the specified VLAN

### MIB Objects

- `vStpMstInstanceTable`
  - `vStpMstInstanceNumber`
  - `vStpMstInstanceName`
  - `vStpMstInstanceVlanBitmapState`
show spantree cist vlan-map

Displays the range of VLANs associated with the flat mode Common and Internal Spanning Tree (CIST) instance.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.

Examples

-> show spantree cist vlan-map

Cist
Name      : CIST1,
VLAN list : 1-9,14-4094

output definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>An alphanumeric value that identifies the name of the CIST. Use the <code>spantree msti</code> command to define a name for this instance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN list</td>
<td>The range of VLAN IDs that are associated with the CIST instance.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Distributed Spanning Tree Commands

Related Commands

**show spantree mst**
Displays the MST region information for the switch.

**show spantree msti vlan-map**
Displays the range of VLANs associated to the specified MSTI.

**show spantree map-msti**
Displays the MSTI that is associated to the specified VLAN

MIB Objects

`vStpMstInstanceTable`
- `vStpMstInstanceNumber`
- `vStpMstInstanceName`
- `vStpMstInstanceVlanBitmapState`
show spantree map-msti

Displays the Multiple Spanning Tree Instance (MSTI) that is associated to the specified VLAN.

show spantree [vlan vlan_id] map-msti

Syntax Definitions

vlan_id An existing VLAN ID number.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is available when the switch is operating in either the per-VLAN or flat Spanning Tree mode.
- Initially all VLANs are associated with the flat mode CIST instance.

Examples

-> show spantree map-msti

Vlan Msti/Cist(0)
----------+------------------------
  200     1

Release History

Release 7.1.1; command introduced.
Related Commands

- `show spantree mst` Displays the MST region information for the switch.
- `show spantree msti vlan-map` Displays the range of VLANs associated to the specified MSTI.
- `show spantree cist vlan-map` Displays the range of VLANs associated to the CIST instance.

MIB Objects

`vStpMstVlanAssignmentTable`

- `vStpMstVlanAssignmentVlanNumber`
- `vStpMstVlanAssignmentMstiNumber`
9 Shortest Path Bridging Commands

The OmniSwitch supports Shortest Path Bridging MAC (SPBM), as defined in the IEEE 802.1aq standard. SPB-M uses the Provider Backbone Bridge (PBB) network model to encapsulate (using IEEE 802.1ah headers) and tunnel customer traffic through the network backbone. The shortest path trees (SPTs) upon which the PBB network infrastructure operates are determined using a version of the Intermediate System-to-Intermediate System (IS-IS) link state protocol that supports TLV extensions for SPB (ISIS-SPB).

The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free, SPTs through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the 802.1ah MAC-in-MAC method for data encapsulation. SPBM services transport the encapsulated traffic over the ISIS-SPB infrastructure.

This chapter documents the Command Line Interface (CLI) commands used to configure and verify the ISIS-SPB backbone. For commands used to configure and verify the SPBM services layer, see Chapter 10, “Service Manager Commands.”

MIB information for the SPB commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-ISIS-SPB-MIB.mib</td>
<td>alcatelIND1IsisSpbMib</td>
</tr>
<tr>
<td>ALCATEL-IND1-VLAN-MGR-MIB.mib</td>
<td>alcatelIND1VLANMgrMIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>Global SPB Commands</th>
<th>spb isis admin-state</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>spb isis area-address</td>
</tr>
<tr>
<td></td>
<td>spb isis bridge-priority</td>
</tr>
<tr>
<td></td>
<td>spb isis source-id</td>
</tr>
<tr>
<td></td>
<td>spb isis control-address</td>
</tr>
<tr>
<td></td>
<td>spb isis spf-wait</td>
</tr>
<tr>
<td></td>
<td>spb isis lsp-wait</td>
</tr>
<tr>
<td></td>
<td>spb isis rapid-lsp-converge</td>
</tr>
<tr>
<td></td>
<td>spb isis overload</td>
</tr>
<tr>
<td></td>
<td>spb isis overload-on-boot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPB Backbone VLAN (BVLAN) Commands</th>
<th>spb bvlan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>spb isis bvlan ect-id</td>
</tr>
<tr>
<td></td>
<td>spb isis control-bvlan</td>
</tr>
<tr>
<td></td>
<td>spb isis bvlan tandem-multicast-mode</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SPB Interface Commands</th>
<th>spb isis interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPB IP VPN Commands</td>
<td>spb ipvpn bind</td>
</tr>
<tr>
<td></td>
<td>spb ipvpn redist</td>
</tr>
<tr>
<td></td>
<td>show spb ipvpn bind</td>
</tr>
<tr>
<td></td>
<td>show spb ipvpn redist</td>
</tr>
<tr>
<td></td>
<td>show spb ipvpn route-table</td>
</tr>
<tr>
<td>SPB IPv6 VPN Commands</td>
<td>spb ipvpn6 bind</td>
</tr>
<tr>
<td></td>
<td>spb ipvpn6 redist</td>
</tr>
<tr>
<td></td>
<td>show spb ipvpn6 bind</td>
</tr>
<tr>
<td></td>
<td>show spb ipvpn6 redist</td>
</tr>
<tr>
<td></td>
<td>show spb ipvpn6 route-table</td>
</tr>
<tr>
<td>SPB Graceful Restart</td>
<td>spb isis graceful-restart</td>
</tr>
<tr>
<td>Commands</td>
<td>spb isis graceful-restart helper</td>
</tr>
<tr>
<td>SPB Show Commands</td>
<td>show spb isis info</td>
</tr>
<tr>
<td></td>
<td>show spb isis bvlans</td>
</tr>
<tr>
<td></td>
<td>show spb isis interface</td>
</tr>
<tr>
<td></td>
<td>show spb isis adjacency</td>
</tr>
<tr>
<td></td>
<td>show spb isis database</td>
</tr>
<tr>
<td></td>
<td>show spb isis nodes</td>
</tr>
<tr>
<td></td>
<td>show spb isis unicast-table</td>
</tr>
<tr>
<td></td>
<td>show spb isis services</td>
</tr>
<tr>
<td></td>
<td>show spb isis spf</td>
</tr>
<tr>
<td></td>
<td>show spb isis multicast-table</td>
</tr>
<tr>
<td></td>
<td>show spb isis multicast-sources</td>
</tr>
<tr>
<td></td>
<td>show spb isis multicast-sources-spf</td>
</tr>
<tr>
<td></td>
<td>show spb isis ingress-mac-filter</td>
</tr>
<tr>
<td></td>
<td>show spb isis rapid-lsp-converge-info</td>
</tr>
<tr>
<td></td>
<td>show spb isis rapid-lsp-converge-table</td>
</tr>
</tbody>
</table>
**spb bvlan**

Configures an SPB backbone VLAN (BVLAN).

```
spb bvlan {bvlan_id|-bvlan_id2}] [admin-state {enable | disable}] [name description]
```

```no spb bvlan bvlan_id```

**Syntax Definitions**

- `bvlan_id[-bvlan_id2]` A numeric value that uniquely identifies an individual BVLAN. The valid ID range is 1–4094. Use a hyphen to specify a range of BVLAN IDs (10-20).
- `enable` Enables the VLAN administrative status.
- `disable` Disables the VLAN administrative status.
- `description` An alphanumeric string. Optional name description for the VLAN ID.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>`enable</td>
<td>disable`</td>
</tr>
<tr>
<td><code>description</code></td>
<td>VLAN ID</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a BVLAN from the switch configuration. All BVLAN ports are detached before the BVLAN is removed.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with a space in between.
- The BVLAN configuration must be the same on each SPB bridge to ensure proper ISIS-SPB neighbor discovery and shortest path calculations throughout the provider backbone bridge (PBB) network.
- BVLANs differ from standard VLANs as follows:
  - No Spanning Tree control—the Spanning Tree protocol is automatically disabled on each BVLAN, and all ports associated with each BVLAN will remain in a forwarding state. However, Spanning Tree can remain operational on other types of VLANs.
  - No source MAC address learning—normal hardware learning is disabled on BVLANs. Instead, the
forwarding database (FDB) is populated by the ISIS-SPB protocol.

- There is no flooding of unknown destination or multicast frames.
- Ingress filtering based on the source MAC address—frames received on ports that do not have an incoming source MAC address pre-programmed by ISIS-SPB are discarded.

- All BVLANs are automatically associated with all ISIS-SPB interfaces. Adding or removing BVLANs from a specific SPB interface is not allowed.

- The recommended maximum number of BVLANs is four. Keeping the number of BVLANs at four or less reduces the number of address updates across the control plane and helps to improve scalability, stability, and convergence time in the SPB network.

- BVLANs and standard VLANs can co-exist on the same bridge ports.

**Examples**

- `-> spb bvlan 200 name BVLAN-200`
- `-> spb bvlan 720 admin-state disable`
- `-> spb bvlan 500 name BVLAN-500 admin-state enable`
- `-> no spb bvlan 1020`

**Release History**

Release 7.3.1; command introduced.

**Related Commands**

- `spb isis control-bvlan`        Configures a control BVLAN
- `spb isis bvlan ect-id`        Assigns an equal cost tree (ECT) algorithm ID to the specified BVLAN.
- `spb isis bvlan tandem-multicast-mode`        Configures the tandem multicast mode for the specified SPB backbone VLAN (BVLAN).
- `spb isis interface`        Configures ISIS-SPB network interfaces.
- `show spb isis bvlan`        Displays the BVLAN configuration for the switch.

**MIB Objects**

- `vlanTable`
  - `vlanNumber`
  - `vlanDescription`
  - `vlanAdmStatus`
  - `vlanOperStatus`
  - `vlanType`
**spb isis bvlan ect-id**

Configures the equal cost tree (ECT) identifier for the specified SPB backbone VLAN (BVLAN). The ECT ID assigns a tie-breaking algorithm to the BVLAN that is used for shortest path tree (SPT) calculations.

```
spb isis bvlan bvlan_id ect-id ect_id
```

**Syntax Definitions**

- **bvlan_id**
  
  An existing BVLAN ID.

- **ect_id**
  
  An ECT algorithm ID. The valid range is 1–16.

**Defaults**

By default, the next available ECT ID number is automatically assigned to a BVLAN when the BVLAN is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to change the existing ECT ID number for the specified BVLAN on each SPB bridge, as necessary, to make sure the specified BVLAN uses the same ECT ID throughout the network.

- The BVLAN ID specified with this command must already exist in the switch configuration.

**Examples**

```
-> spb isis bvlan 200 ect-id 5
-> spb isis bvlan 720 ect-id 10
```

**Release History**

Release 7.3.1; command introduced.
Related Commands

spb bvlan
Creates a SPB backbone VLAN (BVLAN).

show spb isis bvlans
Displays the SPB BVLAN configuration for the switch.

MIB Objects

alcatelIND1IsisSpbEctStaticTable

alcatelIND1IsisSpbEctStaticEntryBaseVid
spb isis control-bvlan

Designates an existing BVLAN that will serve as the control BVLAN for the bridge. Only one BVLAN per bridge is designated as the control BVLAN, which is used to exchange ISIS-SPB control packets with neighboring SPB bridges on behalf of all the BVLANs configured for that bridge.

spb isis control-bvlan bvlan_id

**Syntax Definitions**

-bvlan_id An existing BVLAN ID.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The BVLAN ID specified with this command must already exist in the switch configuration.
- The control BVLAN ID is the VLAN tag that is applied to ISIS-SPB control frames.
- Configuring an existing BVLAN as the control BVLAN does not exclude that VLAN from carrying data traffic for the SPB domain. In other words, a single VLAN can serve as both a regular BVLAN and the control BVLAN at the same time.

**Examples**

- `> spb isis control-bvlan 200`
- `> spb isis control-bvlan 720`

**Release History**

Release 7.3.1; command introduced.
Related Commands

spb bvlan                          Configures an SPB BVLAN.
show spb isis bvlangs            Displays the BVLAN configuration for the bridge.

MIB Objects

alcatelIND1IsisSpbSys
  alcatelIND1IsisSpbSysControlBvlan
**spb isis bvlan tandem-multicast-mode**

Configures the tandem multicast mode for the specified SPB backbone VLAN (BVLAN). This mode is only applicable to associated SPB service instances that are configured to use the tandem replication mode for multicast traffic.

```
spb isis bvlan bvlan_id tandem-multicast-mode {sgmode | gmode}
```

### Syntax Definitions

- `bvlan_id`: An existing BVLAN ID.
- `sgmode`: Specifies the source and group (S,G) mode for the BVLAN.
- `gmode`: Specifies the any source and group (*,G).

### Defaults

By default, BVLANs are configured to use the (S,G) mode.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The BVLAN ID specified with this command must already exist in the switch configuration.
- The (S,G) mode identifies a source-specific multicast distribution tree.
- The (*,G) mode identifies a shared multicast distribution tree.

### Examples

- `-> spb isis bvlan 200 tandem-multicast-mode gmode`
- `-> spb isis bvlan 720 tandem-multicast-mode sgmode`

### Release History

Release 7.3.1; command introduced.
Related Commands

spb bvlan  Creates a SPB backbone VLAN (BVLAN).
show spb isis bvlan  Displays the SPB BVLAN configuration for the switch.

MIB Objects

alcatelIND1IIsisSpbEctStaticTable
  alcatelIND1IIsisSpbEctStaticEntryBaseVid
  alcatelIND1IIsisSpbEctStaticEntryMulticastMode
**spb isis bridge-priority**

Configures the bridge priority value for the SPB bridge. This value is used to rank an SPB bridge in relation to other bridges.

**spb isis bridge-priority priority**

---

**Syntax Definitions**

*priority* A bridge priority value. The valid range is 0–65535.

**Defaults**

By default, the bridge priority value for the switch is set to 32768.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The lower the bridge priority number assigned, the higher the priority that is associated with the bridge.
- The bridge priority value makes up the upper two bytes of the eight-byte SPB bridge ID. The lower six bytes of the Bridge ID contain the system ID, which is the dedicated bridge MAC address of the SPB bridge.
- Setting a different bridge priority value on different SPB bridges will override the system identifier significance during the shortest path tree (SPT) calculation.

**Examples**

- `--> spb isis bridge-priority 15`
- `--> spb isis bridge-priority 32768`

**Release History**

Release 7.3.1; command introduced.
Related Commands

show spb isis info      Displays the status and configuration information for the SPB bridge.

MIB Objects

alcatelIND1IsisSpbSys
  alcatelIND1IsisSpbSysBridgePriority
spb isis interface

Configures the specified port or link aggregate as an ISIS-SPB interface on which protocol data units (PDUs) are sent and received to detect neighbors and form adjacencies with other SPB bridges in the network.

```
spb isis interface {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [admin-state {enable | disable}] [hello-interval seconds] [hello-multiplier count] [metric metric] [type {p2p | multi-access}] [priority priority]
```

```
no spb isis interface {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **enable**: Administratively enables the SPB interface.
- **disable**: Administratively disables the SPB interface.
- **seconds**: The amount of time, in seconds, to wait between each transmission of a hello packet from this interface. The valid range is 1–20000.
- **count**: An integer value that is multiplied by the hello interval time to determine the amount of time, in seconds, a receiving bridge holds onto the hello packets transmitted from this interface. The valid range is 2–100.
- **metric**: An integer value that specifies the link cost to reach the destination BMAC. The valid range is 1–16777215.
- **p2p**: Configures the interface as an SPB point-to-point interface (P2P) on which one adjacency is allowed.
- **multi-access**: Configures the interface as an SPB multiple access LAN interface on which multiple adjacencies are allowed.
- **priority**: The priority value assigned to the ISIS-SPB interface. The valid range is 1–127. This value applies only when the interface is configured as an SPB multiple access LAN interface.
Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>seconds</td>
<td>9 (p2p)</td>
</tr>
<tr>
<td>count</td>
<td>3</td>
</tr>
<tr>
<td>metric</td>
<td>10</td>
</tr>
<tr>
<td>p2p</td>
<td>multi-access</td>
</tr>
<tr>
<td>priority</td>
<td>64</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the ISIS-SPB interface.
- When configuring a link aggregate as an SPB interface, make sure the link aggregate ID number already exists in the switch configuration.
- All SPB interfaces are automatically assigned to all existing BVLANs. There is one ISIS-SPB instance per switch, and each BVLAN and SPB interface is associated with that instance.
- If the SPB interface metric value is set to a different value for each side of a link, the highest metric value is applied to the entire link.
- Administratively enabling ISIS-SPB on the switch, triggers IS-IS hello packet transmissions on all SPB interfaces.
- Configuring a port or link aggregate as an SPB multiple access (multi-access) LAN interface allows multiple adjacencies to form on that interface. This is particularly useful for extending an SPB backbone over a shared Ethernet domain, such as a shared service provider network or even connect to another ISIS-SPB domain.

Note. Software releases prior to AOS Release 8.7R1 do not process pseudo-node LSPs generated by multi-access interfaces. As a result, SPB nodes running such software may experience inconsistent connectivity to destinations beyond the shared Ethernet network segment. If such network reachability is desired, those SPB nodes must be upgraded to AOS Release 8.7R1.

- Consider the following when an interface is configured as an SPB multi-access interface:
  - LAN IS-IS Hello (IIH) packets containing a priority value and a LAN ID (System ID plus a unique local Circuit ID) are exchanged between multi-access LAN interfaces to discover neighbors and form adjacencies over a shared network.
A Designated Intermediate System (DIS) election process determines which multi-access LAN interface will serve as the DIS for the network. A DIS is elected based on which interface has the highest configurable priority value, with the highest backbone MAC address (BMAC) used as a tiebreaker.

All multi-access LAN interfaces report their adjacencies to the DIS. The DIS represents all of the multi-access links as a virtual SPB node (pseudo-node) to IS-IS by generating a pseudo-node LSP. This type of LSP contains a list all the multi-access links, including the DIS, that comprise the virtual SPB node.

The DIS is responsible for synchronizing the LSP database across a shared, multiple access network and calculating the shortest path through the shared network. All shortest paths calculated travel through the DIS.

The shared network (such as a service provider network) serves as the core over which an SPB multiple access domain is configured. Backbone Edge Bridges (BEBs) connect to the shared network instead of Backbone Core Bridges (BCB).

Configuring an SPB P2P interface and an SPB multi-access LAN interface on the same switch is supported.

- SPB interfaces are typically the Network Network Interface (NNI) ports that carry encapsulated customer data traffic through the Provider Backbone Bridge (PBB) network.
- Note that configuring a port or link aggregate as an SPB interface does not prevent configuration of other VLAN tagging on that port. In other words, the SPB interface can forward regular traffic for other VLAN types in addition to encapsulated SPBM traffic.

**Examples**

-> spb isis interface port 1/4/7
-> spb isis interface port 1/4/7 hello-interval 60
-> spb isis interface linkagg 3
-> spb isis interface linkagg 3 hello-multiplier 10
-> spb isis interface port 1/1/10 hello-interval 20 hello-multiplier 5 metric 2
-> no spb isis interface port 1/4/7
-> no spb isis interface linkagg 3

-> spb isis interface port 1/4/7 type multi-access
-> spb isis interface port 1/4/7 type p2p
-> spb isis interface linkagg 3 type multi-access
-> spb isis interface linkagg 3 type p2p

**Release History**

Release 7.3.1; command introduced.
Release 8.7R1; p2p, multi-access, and priority parameters added.

**Related Commands**

*show spb isis interface* Displays the ISIS-SPB interface configuration for the bridge.
**MIB Objects**

```plaintext
alcatelIND1IsisSpbAdjStaticTable
  alcatelIND1IsisSpbAdjStaticEntryIfIndex
  alcatelIND1IsisSpbAdjStaticEntryMetric
  alcatelIND1IsisSpbAdjStaticEntryHelloInterval
  alcatelIND1IsisSpbAdjStaticEntryHelloMultiplier
  alcatelIND1IsisSpbAdjStaticEntryIfAdminState
  alcatelIND1IsisSpbAdjStaticEntryIfType
  alcatelIND1IsisSpbAdjStaticEntryIfPriority
  alcatelIND1IsisSpbAdjStaticEntryIfCsnpInterval
  alcatelIND1IsisSpbAdjStaticEntryIfNumAdjacencies
  alcatelIND1IsisSpbAdjStaticEntryIfDis
```
**spb ipvpn bind**

Binds a virtual routing and forwarding (VRF) instance, a Shortest Path Bridging (SPB) service instance identifier (ISID), and an IP gateway together to enable the bidirectional exchange of routes between the VRF and SPB ISID via the Global Route Manager (GRM).

```
spb ipvpn bind vrf {vrf_name | default} isid instance_id gateway ip_address {all-routes | import-route-map route_map_name}

no spb ipvpn bind vrf {vrf_name | default} isid instance_id gateway ip_address
```

### Syntax Definitions

- **vrf_name | default**
  
  The name of an existing VRF instance for which routes are imported from the Global Routing Table (GRT) to ISIS-SPB. Enter `default` to specify the default VRF instance.

- **instance_id**
  
  An existing ISID that identifies a Shortest Path Bridging (SPB) service in a provider backbone bridge (PBB) network.

- **ip_address**
  
  The IPv4 address of an IP interface that is associated with the specified VRF instance.

- **all-routes**
  
  Imports or exports all routes for this bind entry.

- **route_map_name**
  
  The name of an existing route map to use for filtering VRF routes that are imported from the GRT to ISIS-SPB for this bind entry. There is no filtering from ISIS-SPB to the GRT.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the VRF-ISID bind entry. When the bind is deleted, all routes imported and exported for this binding are retracted.

- The specified VRF name, ISID, gateway IP address, and optional route map name must already exist in the local switch configuration. In addition, the specified route map must exist in the default VRF instance.

- Only one ISID can be bound to a single VRF/gateway IP instance.
The VRF-ISID binding is only active when the VRF exists, the ISID is configured on the local switch, and the gateway IP address is associated with an active IP interface that is associated with the VRF instance.

An active "bind" entry causes ISIS-SPB to export learned routes from the SPB network to the GRM and triggers the GRM to send IP routes from the corresponding VRF to ISIS-SPB using the ISID and gateway IP address as the next hop.

A VRF-ISID binding identifies an L3 VPN interface that will exchange routes between the VLAN domain (VRF instance) and the SPB service domain (I-SID). An L3 VPN interface is required when configuring IP routing over SPB. For more information and configuration examples, refer to the “IP over SPB” section of the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

**Examples**

```plaintext
-> spb ipvpn bind vrf1 isid 1000 gateway 10.1.1.1 all-routes
-> spb ipvpn bind vrf2 isid 2000 gateway 20.2.2.1 import-route-map rm_vrf2
-> no spb ipvpn bind vrf1 isid 1000 gateway 10.1.1.1
```

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- `spb ipvpn redist`  
  Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.

- `show spb ipvpn bind`  
  Displays VRF-to-ISID bindings that enable the import and export of routes between VRFs and ISIDs.

**MIB Objects**

- `alcatelIND1IsisSpbIPVPNBindTable`
- `alcatelIND1IsisSpbIPVPNBindVrfName`
- `alcatelIND1IsisSpbIPVPNBindIsid`
- `alcatelIND1IsisSpbIPVPNBindGatewayType`
- `alcatelIND1IsisSpbIPVPNBindGateway`
- `alcatelIND1IsisSpbIPVPNBindImportRouteMap`
- `alcatelIND1IsisSpbIPVPNBindRowStatus`
**spb ipvpn redist**

Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.

```
spb ipvpn redist {source-vrf {vrf_name | default} | source-isid instance_id} destination-isid instance_id {all-routes | route-map route_map_name}
```

```
no spb ipvpn redist {source-vrf vrf_name | source-isid instance_id} destination-isid instance_id
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf_name</td>
<td>default</td>
</tr>
<tr>
<td>source-isid instance_id</td>
<td>The source ISID from which routes are redistributed.</td>
</tr>
<tr>
<td>destination-isid instance_id</td>
<td>The destination ISID to which routes from either the source VRF or source ISD are redistributed.</td>
</tr>
<tr>
<td>all-routes</td>
<td>route_map_name</td>
</tr>
<tr>
<td>route_map_name</td>
<td>The name of an existing route map to use for filtering routes that are redistributed.</td>
</tr>
</tbody>
</table>

** Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the redistribution entry.
- The specified VRF name, ISID, and optional route map name must already exist in the local switch configuration.
- A redistribution entry is only active when the ISID belongs to an active bind entry. This applies to both ISIDs when redistributing between a source and destination ISID.
- An ISID cannot be bound and redistributed to the same VRF instance.
- The difference between a bind entry and a redistribution entry is as follows:
  - A bind entry binds only one I-SID to one VRF/gateway IP instance. IP VPN routes are then imported and exported bidirectionally between the VRF and I-SID.
  - A redistribution entry allows multiple VRFs to redistribute routes into one I-SID. However, IP VPN routes are only redistributed into the I-SID; there is no bidirectional exchange of routes between the
VRF and I-SID. Redistribution is mainly used when routing between I-SIDs is required.

**Examples**

-> spb ipvpn redist source-isid 1000 destination-isid 2000 all-routes
-> spb ipvpn redist source-isid 2000 destination-isid 1000 all-routes
-> spb ipvpn redist source-vrf vrf1 destination-isid 3000 route-map rm_isid2000
-> no spb ipvpn redist source-vrf vrf1 destination-isid 3000
-> no spb ipvpn redist source-isid 2000 destination isid 1000

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

spb ipvpn bind

Binds a VRF instance, an ISID, and an IP gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.

show spb ipvpn redist

Displays the SPB IPVPN redistribution configuration for the switch.

**MIB Objects**

alcatelIND1IsisSpbIPVPNRedistVrfTable
  alcatelIND1IsisSpbIPVPNRedistVrfSourceVrf
  alcatelIND1IsisSpbIPVPNRedistVrfDestIsid
  alcatelIND1IsisSpbIPVPNRedistVrfInetType
  alcatelIND1IsisSpbIPVPNRedistVrfRouteMap
  alcatelIND1IsisSpbIPVPNRedistVrfRowStatus

alcatelIND1IsisSpbIPVPNRedistIsidTable
  alcatelIND1IsisSpbIPVPNRedistIsidSourceIsid
  alcatelIND1IsisSpbIPVPNRedistIsidDestIsid
  alcatelIND1IsisSpbIPVPNRedistIsidInetType
  alcatelIND1IsisSpbIPVPNRedistIsidRouteMap
  alcatelIND1IsisSpbIPVPNRedistIsidRowStatus
**show spb ipvpn bind**

Displays VRF-to-ISID bindings that enable the import and export of routes between VRFs and ISIDs.

```
show spb ipvpn bind [vrf {vrf_name | default}] [isid instance_id]
```

### Syntax Definitions

- **vrf_name | default**: The name of a VRF instance that is associated with an SPB IPVPN binding. Enter `default` to specify the default VRF instance.
- **instance_id**: An ISID number that is associated with an SPB IPVPN binding.

### Defaults

By default, all SPB IPVPN bindings are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `vrf` and `isid` parameters to display the configuration for specific bindings.

### Examples

```
$ -> show spb ipvpn bind
Legend: * indicates bind entry is active
SPB IPVPN Bind Table:
+---------+---------+-----------+----------------+------------------+
| VRF     | ISID    | Gateway   | Route-Map      |
|---------+---------+-----------+----------------+------------------+
| * ospf  | 4001    | 1.1.1.2   |                |
| * ospf1 | 4003    | 2.2.2.2   |                |
```

Total Bind Entries: 2

### Output Definitions

- **VRF**: The name of the VRF instance associated with this binding.
- **ISID**: The ISID number associated with this binding.
- **Gateway**: The gateway IP address associated with this binding. This is the IP address specified for an IP interface that is associated with the VRF in this binding.
- **Route-Map**: The name of an IP route map or All Routes.
Release History

Release 7.3.2; command introduced.

Related Commands

spb ipvpn bind  Binds a VRF instance, an ISID, and an IP gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.

show spb ipvpn redist  Displays the SPB IP VPN redistribution configuration for the switch.

show spb ipvpn route-table Displays the contents of the SPB IPVPN route table.

MIB Objects

alcatelIND1IsisSpbIPVPNBindTable
  alcatelIND1IsisSpbIPVPNBindVrfName
  alcatelIND1IsisSpbIPVPNBindIsid
  alcatelIND1IsisSpbIPVPNBindGatewayType
  alcatelIND1IsisSpbIPVPNBindGateway
  alcatelIND1IsisSpbIPVPNBindRouteMap
show spb ipvpn redist

Displays the SPB IPVPN redistribution configuration for the switch. This configuration controls the redistribution of IP VPN routes from ISID to ISID or from VRF to ISID.

show spb ipvpn redist [vrf | [isid]]

Syntax Definitions

vrf Displays the VRF redistribution table.
isid Displays the ISID redistribution table.

Defaults

By default, both the VRF and ISID redistribution tables are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the isid parameter to display the contents of the ISID redistribution table (ISID to ISID).
- Use the vrf parameter to display the contents of the VRF redistribution table (VRF to ISID).

Examples

-> show spb ipvpn redist
Legend: * indicates redist entry is active
SPB IPVPN Redist ISID Table:

<table>
<thead>
<tr>
<th>Source-ISID</th>
<th>Destination-ISID</th>
<th>Route-Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 4001</td>
<td>4003</td>
<td></td>
</tr>
<tr>
<td>* 4003</td>
<td>4001</td>
<td></td>
</tr>
</tbody>
</table>

Total Redist ISID Entries: 2

Legend: * indicates redist entry is active
SPB IPVPN Redist VRF Table:

<table>
<thead>
<tr>
<th>Source-VRF</th>
<th>Destination-ISID</th>
<th>Route-Map</th>
</tr>
</thead>
</table>

Total Redist Vrf Entries: 0
-> show spb ipvpn redist isid
Legend: * indicates redist entry is active
SPB IPVPN Redist ISID Table:

<table>
<thead>
<tr>
<th>Source-ISID</th>
<th>Destination-ISID</th>
<th>Route-Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 4001</td>
<td>4003</td>
<td></td>
</tr>
<tr>
<td>* 4003</td>
<td>4001</td>
<td></td>
</tr>
</tbody>
</table>

Total Redist ISID Entries: 2

-> show spb ipvpn redist vrf
Legend: * indicates redist entry is active
SPB IPVPN Redist VRF Table:

<table>
<thead>
<tr>
<th>Source-VRF</th>
<th>Destination-ISID</th>
<th>Route-Map</th>
</tr>
</thead>
</table>

Total Redist Vrf Entries: 0

**Output definitions**

<table>
<thead>
<tr>
<th>Source-ISID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The ISID number from which routes are redistributed to the destination ISID.</td>
</tr>
<tr>
<td>Source-VRF</td>
<td>The name of the VRF instance from which routes are redistributed to the destination ISID.</td>
</tr>
<tr>
<td>Destination-ISID</td>
<td>The ISID number to which routes are redistributed from another ISID or from a VRF instance.</td>
</tr>
<tr>
<td>Route-Map</td>
<td>The name of an IP route map that is used to filter the redistributed routes.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- **spb ipvpn redist**  Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.
- **show spb ipvpn bind**  Displays the VRF-ISID binding configuration.
- **show spb ipvpn route-table**  Displays the contents of the SPB IPVPN route table.

**MIB Objects**

- `alcatelIND1IsisSpbIPVPNRedistIsidTable`
- `alcatelIND1IsisSpbIPVPNRedistIsidSourceIsid`
- `alcatelIND1IsisSpbIPVPNRedistIsidDestIsid`
- `alcatelIND1IsisSpbIPVPNRedistRouteMap`
- `alcatelIND1IsisSpbIPVPNRedistVrfTable`
- `alcatelIND1IsisSpbIPVPNRedistVrfSourceVrf`
- `alcatelIND1IsisSpbIPVPNRedistVrfDestIsid`
- `alcatelIND1IsisSpbIPVPNRedistRouteMap`
show spb ipvpn route-table

Displays the contents of the SPB IPVPN route table.

show spb ipvpn route-table [isid instance_id]

**Syntax Definitions**

*instance_id* An ISID number.

**Defaults**

By default, all routes for all ISIDs are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the *isid* parameter to display information for specific ISID routes.

**Examples**

-> show spb ipvpn route-table
Legend: * indicates IPVPN route has matching locally configured ISID

SPB IPVPN Route Table:

<table>
<thead>
<tr>
<th>ISID</th>
<th>Destination</th>
<th>Gateway</th>
<th>Source Bridge (Name : BMAC)</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>4001 1.1.1.0/24</td>
<td>1.1.1.1</td>
<td>L2-DUT1 : 00:e0:b1:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 1.1.1.0/24</td>
<td>1.1.1.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2.2.2.0/24</td>
<td>1.1.1.1</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 10.10.10.0/24</td>
<td>1.1.1.1</td>
<td>L2-DUT1 : 00:e0:b1:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 15.1.1.0/24</td>
<td>1.1.1.1</td>
<td>L2-DUT1 : 00:e0:b1:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 15.1.2.0/24</td>
<td>1.1.1.1</td>
<td>L2-DUT1 : 00:e0:b1:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 15.1.3.0/24</td>
<td>1.1.1.1</td>
<td>L2-DUT1 : 00:e0:b1:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 15.1.4.0/24</td>
<td>1.1.1.1</td>
<td>L2-DUT1 : 00:e0:b1:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 15.1.5.0/24</td>
<td>1.1.1.1</td>
<td>L2-DUT1 : 00:e0:b1:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 20.20.20.0/24</td>
<td>1.1.1.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 25.1.1.0/24</td>
<td>1.1.1.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 25.1.2.0/24</td>
<td>1.1.1.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 25.1.3.0/24</td>
<td>1.1.1.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 25.1.4.0/24</td>
<td>1.1.1.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 25.1.5.0/24</td>
<td>1.1.1.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4003 1.1.1.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4003 2.2.2.0/24</td>
<td>2.2.2.1</td>
<td>L2-DUT2 : 00:e0:b1:dd:99:db</td>
<td>1</td>
</tr>
<tr>
<td>ISID</td>
<td>Destination</td>
<td>Gateway</td>
<td>Source Bridge</td>
<td>Metric</td>
</tr>
<tr>
<td>------</td>
<td>----------------</td>
<td>--------------------------</td>
<td>---------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>4003</td>
<td>2.2.2.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>10.10.10.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>15.1.1.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>15.1.2.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>15.1.3.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>15.1.4.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>15.1.5.0/24</td>
<td>2.2.2.2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>20.20.20.0/24</td>
<td>2.2.2.1</td>
<td>L2-DUT2 : 00:e0:b1:dd:99:db</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>25.1.1.0/24</td>
<td>2.2.2.1</td>
<td>L2-DUT2 : 00:e0:b1:dd:99:db</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>25.1.2.0/24</td>
<td>2.2.2.1</td>
<td>L2-DUT2 : 00:e0:b1:dd:99:db</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>25.1.3.0/24</td>
<td>2.2.2.1</td>
<td>L2-DUT2 : 00:e0:b1:dd:99:db</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>25.1.4.0/24</td>
<td>2.2.2.1</td>
<td>L2-DUT2 : 00:e0:b1:dd:99:db</td>
<td>1</td>
</tr>
<tr>
<td>4003</td>
<td>25.1.5.0/24</td>
<td>2.2.2.1</td>
<td>L2-DUT2 : 00:e0:b1:dd:99:db</td>
<td>1</td>
</tr>
</tbody>
</table>

Routes: 30

**output definitions**

- **ISID**: The ISID number associated with this route.
- **Destination**: Destination IP address. Also includes the prefix length notation after the address to indicate the number of bits that are significant in the IPv6 address (mask).
- **Gateway**: IP address of the gateway from which this route was learned.
- **Source Bridge (Name : BMAC)**: The name and BMAC address of the SPB BEB switch that advertised the route.
- **Metric**: The metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- `show spb ipvpn redist`: Displays the SPB IPVPN redistribution configuration for the switch.
- `show spb ipvpn bind`: Displays the VRF-ISID binding configuration.

**MIB Objects**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alcatelIND1IsisSpbIPVPNRouteTable</td>
<td></td>
</tr>
<tr>
<td>alcatelIND1IsisSpbIPVPNRouteIsid</td>
<td></td>
</tr>
<tr>
<td>alcatelIND1IsisSpbIPVPNRoutePrefixType</td>
<td></td>
</tr>
<tr>
<td>alcatelIND1IsisSpbIPVPNRoutePrefix</td>
<td></td>
</tr>
<tr>
<td>alcatelIND1IsisSpbIPVPNRoutePrefixLen</td>
<td></td>
</tr>
<tr>
<td>alcatelIND1IsisSpbIPVPNRouteGateway</td>
<td></td>
</tr>
<tr>
<td>alcatelIND1IsisSpbIPVPNRouteNodeName</td>
<td></td>
</tr>
<tr>
<td>alcatelIND1IsisSpbIPVPNRouteMetric</td>
<td></td>
</tr>
</tbody>
</table>
**spb ipv6 bind**

Binds a virtual routing and forwarding (VRF) instance, a Shortest Path Bridging (SPB) service instance identifier (ISID), and an IPv6 gateway together to enable the bidirectional exchange of routes between the VRF and SPB ISID via the Global Route Manager (GRM).

```
spb ipv6 bind vrf {vrf_name | default} isid instance_id gateway ipv6_address {all-routes | import-route-map route_map_name}
```

```
no spb ipv6 bind vrf {vrf_name | default} isid instance_id gateway ipv6_address
```

**Syntax Definitions**

- `vrf_name | default`: The name of an existing VRF instance for which routes are imported from the Global Routing Table (GRT) to ISIS-SPB. Enter `default` to specify the default VRF instance.
- `instance_id`: An existing ISID that identifies a Shortest Path Bridging (SPB) service in a provider backbone bridge (PBB) network.
- `ipv6_address`: The IPv6 address of an IPv6 interface that is associated with the specified VRF instance.
- `all-routes`: Imports or exports all routes for this bind entry.
- `route_map_name`: The name of an existing route map to use for filtering VRF routes that are imported from the GRT to ISIS-SPB for this bind entry. There is no filtering from ISIS-SPB to the GRT.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the VRF-ISID bind entry. When the bind is deleted, all routes imported and exported for this binding are retracted.

- The specified VRF name, ISID, gateway IPv6 address, and optional route map name must already exist in the local switch configuration. In addition, the specified route map must exist in the default VRF instance.

- Only one ISID can be bound to a single VRF/gateway IPv6 instance.
The VRF-ISID binding is only active when the VRF exists, the ISID is configured on the local switch, and the gateway IPv6 address is associated with an active IPv6 interface that is associated with the VRF instance.

An active "bind" entry causes ISIS-SPB to export learned routes from the SPB network to the GRM and triggers the GRM to send IPv6 routes from the corresponding VRF to ISIS-SPB using the ISID and gateway IPv6 address as the next hop.

A VRF-ISID binding identifies an L3 VPN interface that will exchange routes between the VLAN domain (VRF instance) and the SPB service domain (I-SID). An L3 VPN interface is required when configuring IPv6 routing over SPB. For more information and configuration examples, refer to the “IP over SPB” section of the “Configuring Shortest Path Bridging” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide.

**Examples**

```bash
-> spb ipv6 bind vrf1 isid 1000 gateway 1000::1 all-routes
-> spb ipv6 bind vrf2 isid 2000 gateway 2000::1 import-route-map rm_vrf2
-> no spb ipv6 bind vrf1 isid 1000 gateway 1000::1
```

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- **spb ipv6 redist**  
  Configures the redistribution of routes from a VRF to an ISID or from one ISID to another ISID.

- **show spb ipv6 bind**  
  Displays VRF-to-ISID bindings that enable the import and export of routes between VRFs and ISIDs.

**MIB Objects**

- alcatelIND1IsisSpbIPVPNBindTable
- alcatelIND1IsisSpbIPVPNBindVrfName
- alcatelIND1IsisSpbIPVPNBindIsid
- alcatelIND1IsisSpbIPVPNBindGatewayType
- alcatelIND1IsisSpbIPVPNBindGateway
- alcatelIND1IsisSpbIPVPNBindImportRouteMap
- alcatelIND1IsisSpbIPVPNBindRowStatus
**spb ipv6 redist**

Configures the redistribution of IPv6 routes from a VRF to an ISID or from one ISID to another ISID.

```
spb ipv6 redist {source-vrf {vrf_name | default} | source-isid instance_id} destination-isid instance_id {all-routes | route-map route_map_name}
```

```
no spb ipv6 redist {source-vrf vrf_name | source-isid instance_id} destination-isid instance_id
```

### Syntax Definitions

| **vrf_name | default** | The source VRF instance from which routes are redistributed. Enter default to specify the default VRF instance. |
| source-isid instance_id | The source ISID from which routes are redistributed. |
| destination-isid instance_id | The destination ISID to which routes from either the source VRF or source ISD are redistributed. |
| all-routes | Imports or exports all routes for this bind entry. |
| route_map_name | The name of an existing route map to use for filtering routes that are redistributed. |

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the redistribution entry.
- The specified VRF name, ISID, and optional route map name must already exist in the local switch configuration.
- A redistribution entry is only active when the ISID belongs to an active bind entry. This applies to both ISIDs when redistributing between a source and destination ISID.
- An ISID cannot be bound and redistributed to the same VRF instance.
- The difference between a bind entry and a redistribution entry is as follows:
  - A bind entry binds only one I-SID to one VRF/IPv6 gateway instance. IPv6 VPN routes are then imported and exported bidirectionally between the VRF and I-SID.
  - A redistribution entry allows multiple VRFs to redistribute routes into one I-SID. However, IPv6 VPN routes are only redistributed into the I-SID; there is no bidirectional exchange of routes.
between the VRF and I-SID. Redistribution is mainly used when routing between I-SIDs is required.

**Examples**

- `-> spb ipv6 redist source-isid 1000 destination-isid 2000 all-routes`
- `-> spb ipv6 redist source-isid 2000 destination-isid 1000 all-routes`
- `-> spb ipv6 redist source-vrf vrf1 destination-isid 3000 route-map rm_isid2000`
- `-> no spb ipv6 redist source-vrf vrf1 destination-isid 3000`
- `-> no spb ipv6 redist source-isid 2000 destination-isid 1000`

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- **spb ipv6 bind**
  Binds a VRF instance, an ISID, and an IPv6 gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.

- **show spb ipv6 redist**
  Displays the SPB IPv6 VPN redistribution configuration for the switch.

**MIB Objects**

- `alcatelIND1IsisSpbIPVPNRedistIsidTable`
- `alcatelIND1IsisSpbIPVPNRedistIsidSourceIsid`
- `alcatelIND1IsisSpbIPVPNRedistIsidDestIsid`
- `alcatelIND1IsisSpbIPVPNRedistIsidInetType`
- `alcatelIND1IsisSpbIPVPNRedistIsidRouteMap`
- `alcatelIND1IsisSpbIPVPNRedistIsidRowStatus`

- `alcatelIND1IsisSpbIPVPNRedistVrfTable`
- `alcatelIND1IsisSpbIPVPNRedistVrfSourceVrf`
- `alcatelIND1IsisSpbIPVPNRedistVrfDestIsid`
- `alcatelIND1IsisSpbIPVPNRedistVrfInetType`
- `alcatelIND1IsisSpbIPVPNRedistVrfRouteMap`
- `alcatelIND1IsisSpbIPVPNRedistVrfRowStatus`
**show spb ipv6 bind**

Displays VRF-to-ISID bindings that enable the import and export of IPv6 routes between VRFs and ISIDs.

`show spb ipv6 bind [vrf {vrf_name | default}] [isid instance_id]`

---

**Syntax Definitions**

- **vrf_name | default**
The name of a VRF instance that is associated with an SPB IPv6 VPN binding. Enter `default` to specify the default VRF instance.

- **instance_id**
An ISID number that is associated with an SPB IPv6 VPN binding.

**Defaults**

By default, all SPB IPv6 VPN bindings are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `vrf` and `isid` parameters to display the configuration for specific bindings.

**Examples**

```
-> show spb ipv6 bind
Legend: * indicates bind entry is active
SPB IPVPN Bind Table:

+---------------------+------------+---------------------+---------------------+
| VRF   | ISID      | Gateway             | Route-Map           |
+---------------------+------------+---------------------+---------------------+
| * ospf              | 4001       | 1000::1             |                     |
| * ospf1             | 4003       | 2000::1             |                     |
+---------------------+------------+---------------------+---------------------+

Total Bind Entries: 2
```

**Output definitions**

- **VRF**
The name of the VRF instance associated with this binding.

- **ISID**
The ISID number associated with this binding.

- **Gateway**
The gateway IPv6 address associated with this binding. This is the IPv6 address configured for an IPv6 interface that is associated with the VRF in this binding.

- **Route-Map**
The name of an IPv6 route map or All Routes.
**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- **spb ipv6 bind**
  Binds a VRF instance, an ISID, and an IPv6 gateway together to enable the bidirectional exchange of routes between the VRF and ISID via the GRM.

- **show spb ipv6 redist**
  Displays the SPB IPv6 VPN redistribution configuration for the switch.

- **show spb ipv6 route-table**
  Displays the contents of the SPB IPv6 VPN route table.

**MIB Objects**

alcatelIND1IsisSpbIPVPNBindTable
  - alcatelIND1IsisSpbIPVPNBindVrfName
  - alcatelIND1IsisSpbIPVPNBindIsid
  - alcatelIND1IsisSpbIPVPNBindGatewayType
  - alcatelIND1IsisSpbIPVPNBindGateway
  - alcatelIND1IsisSpbIPVPNBindRouteMap
show spb ipv6 redist

Displays the SPB IPv6 VPN redistribution configuration for the switch. This configuration controls the redistribution of IPv6 VPN routes from ISID to ISID or from VRF to ISID.

show spb ipv6 redist [vrf | [isid]]

Syntax Definitions

vrf Displays the VRF redistribution table.

isid Displays the ISID redistribution table.

Defaults

By default, both the VRF and ISID redistribution tables are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>6900 X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ISID</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **isid** parameter to display the contents of the ISID redistribution table (ISID to ISID).
- Use the **vrf** parameter to display the contents of the VRF redistribution table (VRF to ISID).

Examples

```- show spb ipv6 redist
Legend: * indicates redist entry is active
SPB IPv6 Redist ISID Table:
Source-ISID Destination-ISID Route-Map
---------------------------------------------+
* 4001 4003
* 4003 4001

Total Redist ISID Entries: 2
Legend: * indicates redist entry is active
SPB IPv6 Redist VRF Table:
Source-VRF Destination-ISID Route-Map
---------------------------------------------+

Total Redist Vrf Entries: 0```

vrf Displays the VRF redistribution table.
isid Displays the ISID redistribution table.
-> show spb ipv6 redist isid
Legend: * indicates redist entry is active
SPB IPVPN Redist ISID Table:
Source-ISID    Destination-ISID     Route-Map
-----------------+--------------------+-----------------
* 4001          4003
* 4003          4001

Total Redist ISID Entries: 2
-> show spb ipv6 redist vrf
Legend: * indicates redist entry is active
SPB IPVPN Redist VRF Table:
Source-VRF            Destination-ISID     Route-Map
---------------------+--------------------+-----------------
Total Redist Vrf Entries: 0

output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-ISID</td>
<td>The ISID number from which IPv6 routes are redistributed to the destination ISID.</td>
</tr>
<tr>
<td>Source-VRF</td>
<td>The name of the VRF instance from which IPv6 routes are redistributed to the destination ISID.</td>
</tr>
<tr>
<td>Destination-ISID</td>
<td>The ISID number to which IPv6 routes are redistributed from another ISID or from a VRF instance.</td>
</tr>
<tr>
<td>Route-Map</td>
<td>The name of an IPv6 route map that is used to filter the redistributed routes.</td>
</tr>
</tbody>
</table>

Release History

Release 8.5R2; command introduced.

Related Commands

spb ipv6 redist  Configures the redistribution of IPv6 routes from a VRF to an ISID or from one ISID to another ISID.
show spb ipv6 bind  Displays the VRF-ISID binding configuration.
show spb ipv6 route-table  Displays the contents of the SPB IPv6 VPN route table.

MIB Objects

alcatelIND1IsisSphIPv6PRedistIsidTable
  alcatelIND1IsisSphIPv6PRedistIsidSourceIsid
  alcatelIND1IsisSphIPv6PRedistIsidDestIsid
  alcatelIND1IsisSphIPv6PRedistRouteMap
alcatelIND1IsisSphIPv6PRedistVrfTable
  alcatelIND1IsisSphIPv6PRedistVrfSourceVrf
  alcatelIND1IsisSphIPv6PRedistVrfDestIsid
  alcatelIND1IsisSphIPv6PRedistRouteMap
show spb ipv6n6 route-table

Displays the contents of the SPB IPv6 VPN route table.

show spb ipv6n6 route-table [isid instance_id]

**Syntax Definitions**

*instance_id*  
An ISID number.

**Defaults**

By default, all IPv6 routes for all ISIDs are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the *isid* parameter to display information for specific ISID routes.

**Examples**

`-> show spb ipv6n6 route-table`

Legend: * indicates IPv6n6 route has matching locally configured ISID

<table>
<thead>
<tr>
<th>ISID</th>
<th>Destination</th>
<th>Gateway</th>
<th>Source Bridge (Name : BMAC)</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>4001 1501::0001::/32</td>
<td>1000::1</td>
<td>L2-DUT1 : 00:e0:bl:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 1601::0001::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 1701::0001::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 1901::0001::/32</td>
<td>1000::1</td>
<td>L2-DUT1 : 00:e0:bl:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2708:3455::/32</td>
<td>1000::1</td>
<td>L2-DUT1 : 00:e0:bl:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2708:3456::/32</td>
<td>1000::1</td>
<td>L2-DUT1 : 00:e0:bl:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2708:3457::/32</td>
<td>1000::1</td>
<td>L2-DUT1 : 00:e0:bl:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2708:3458::/32</td>
<td>1000::1</td>
<td>L2-DUT1 : 00:e0:bl:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2708:3459::/32</td>
<td>1000::1</td>
<td>L2-DUT1 : 00:e0:bl:db:c3:65</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2801::0001::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2901::0001::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2901::0002::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2901::0003::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2901::0004::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4001 2901::0005::/32</td>
<td>1000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4003 1501::0001::/32</td>
<td>2000::2</td>
<td>L2-DEV1 : e8:e7:32:00:23:f9</td>
<td>1</td>
</tr>
<tr>
<td>*</td>
<td>4003 1601::0001::/32</td>
<td>2000::1</td>
<td>L2-DUT2 : 00:e0:bl:dd:99:db</td>
<td>1</td>
</tr>
</tbody>
</table>
* 4003 1701:0001::/32 2000::2 L2-DEV1 : e8:e7:32:00:23:f9 1
* 4003 1901:0001::/32 2000::2 L2-DEV1 : e8:e7:32:00:23:f9 1
* 4003 2708:3455::/32 2000::2 L2-DEV1 : e8:e7:32:00:23:f9 1
* 4003 2708:3456::/32 2000::2 L2-DEV1 : e8:e7:32:00:23:f9 1
* 4003 2708:3457::/32 2000::2 L2-DEV1 : e8:e7:32:00:23:f9 1
* 4003 2708:3458::/32 2000::2 L2-DEV1 : e8:e7:32:00:23:f9 1
* 4003 2708:3459::/32 2000::2 L2-DEV1 : e8:e7:32:00:23:f9 1
* 4003 2801:0001::/32 2000::1 L2-DUT2 : 00:e0:b1:dd:99:db 1
* 4003 2901:0001::/32 2000::1 L2-DUT2 : 00:e0:b1:dd:99:db 1
* 4003 2901:0002::/32 2000::1 L2-DUT2 : 00:e0:b1:dd:99:db 1
* 4003 2901:0003::/32 2000::1 L2-DUT2 : 00:e0:b1:dd:99:db 1
* 4003 2901:0004::/32 2000::1 L2-DUT2 : 00:e0:b1:dd:99:db 1
* 4003 2901:0005::/32 2000::1 L2-DUT2 : 00:e0:b1:dd:99:db 1

Routes: 30

**output definitions**

<table>
<thead>
<tr>
<th>ISID</th>
<th>The ISID number associated with this route.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Destination IPv6 address. Also includes the prefix length notation after the address to indicate the number of bits that are significant in the IPv6 address (mask).</td>
</tr>
<tr>
<td>Gateway</td>
<td>IPv6 address of the gateway from which this route was learned.</td>
</tr>
<tr>
<td>Source Bridge</td>
<td>The name and BMAC address of the SPB BEB switch that advertised the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- `show spb ipv66 redist` Displays the SPB IPv6 VPN redistribution configuration for the switch.
- `show spb ipv66 bind` Displays the VRF-ISID binding configuration.

**MIB Objects**

- `alcatelIND1IsisSpbIPVPNRouteTable`
- `alcatelIND1IsisSpbIPVPNRouteIsid`
- `alcatelIND1IsisSpbIPVPNRoutePrefixType`
- `alcatelIND1IsisSpbIPVPNRoutePrefix`
- `alcatelIND1IsisSpbIPVPNRoutePrefixLen`
- `alcatelIND1IsisSpbIPVPNRouteGateway`
- `alcatelIND1IsisSpbIPVPNRouteNodeName`
- `alcatelIND1IsisSpbIPVPNRouteMetric`
spb isis admin-state

Enables or disables the administrative status of ISIS-SPB instance for the switch.

```
spb isis admin-state {enable | disable}
```

**Syntax Definitions**

- **enable**: Administratively enables ISIS-SPB for the switch.
- **disable**: Administratively disables ISIS-SPB for the switch.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the ISIS-SPB status is disabled, the configuration settings and related statistics of the protocol remain unaffected.

**Examples**

```
-> spb isis admin-state enable
-> spb isis admin-state disable
```

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show spb isis info`: Displays status and configuration information for the SPB instance.

**MIB Objects**

- `alcatelIND1IsisSpbSys`
- `alcatelIND1IsisSpbSysAdminState`
**spb isis area-address**

Configures the area address for the ISIS-SPB instance.

```
spb isis area-address area_address
```

### Syntax Definitions

- **area_address**: A 3-byte integer that specifies the ISIS-SPB area address to join.

### Defaults

By default, the area address is set to 0.0.0. for ISIS-SPB.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The area address is entered in decimal format with this command but is converted and sent out as a hex value on the wire. For example, if the decimal value entered is “73.00.00”, then the hex value actually sent out on the wire is “49.00.00”.
- The default setting of 0.0.0 is the area address typically used for ISIS-SPB.
- Changing the area address with this command is allowed, but make sure to configure each bridge that will participate in the ISIS-SPB instance with the same area address value.
- ISIS-SPB and ISIS-IP instances may co-exist on the same bridge.

### Examples

```
-> spb isis area-address 1.1.1
-> spb isis area-address 0.0.0
```

### Release History

Release 7.3.1; command was introduced.
**Related Commands**

`show spb isis info`  
Displays status and configuration information for the SPB instance.

**MIB Objects**

`alcatelIND1IsisSpbSys`  
`alcatelIND1IsisSpbSysAreaAddress`
**spb isis source-id**

Configures the shortest path (SP) source identifier value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in multicast tandem replication mode.

```
spb isis source-id {source_id | auto}
```

---

**Syntax Definitions**

- **source_id**: A source identifier entered as xx-xx-xx, where xx is a hexadecimal value.
- **auto**: Changes the source ID back to the default value.

---

**Defaults**

By default, the last three least significant bytes of the system ID is used for the source ID.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The source ID is the high order 3 bytes for the Group Address DA for the SPB bridge. Note that only 20 bits are used; the top 4 bits are not used.

---

**Examples**

- `-> spb isis source-id 00-2a-1d`
- `-> spb isis source-id 07-0b-d3`
- `-> spb isis source-id auto`

---

**Release History**

Release 7.3.1; command introduced.

---

**Related Commands**

- `show spb isis info`: Displays status and configuration information for the SPB instance.

---

**MIB Objects**

- `alcatelIND1IsisSpbSys`
- `alcatelIND1IsisSpbmSysSPSourceId`
**spb isis control-address**

Changes the ISIS-SPB control MAC address, which is used as the destination address for ISIS-SPB control packets.

```
spb isis control-address {alll1 | alll2 | allis}
```

### Syntax Definitions

- **alll1**: All Level 1 Intermediate Systems (01:80:C2:00:00:14).
- **alll2**: All Level 2 Intermediate Systems (01:80:C2:00:00:15).
- **allis**: All Intermediate Systems (09:00:2B:00:00:05).

### Defaults

By default, the control MAC address is set to AllL1.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Changing the ISIS-SPB control MAC address on the OmniSwitch can enhance interoperability with third-party ISIS-SPB devices.

### Examples

```
-> spb isis control-address alll1
-> spb isis control-address alll2
-> spb isis control-address allis
```

### Release History

Release 7.3.2; command introduced.
**Related Commands**

*show spb isis info* Displays the status and configuration information for the SPB instance.

**MIB Objects**

- *alcatelIND1IsisSpbSys*
  - *alcatelIND1IsisSpbSysControlAddr*
**spb isis spf-wait**

Configures the time intervals between the first, second, and subsequent ISIS-SPB shortest path first (SPF) calculations.

```
spb isis spf-wait [initial-wait milliseconds | second-wait milliseconds] max-wait milliseconds]
```

**Syntax Definitions**

- **initial-wait milliseconds**
  Specifies the number of milliseconds to wait before triggering an initial SPF calculation after a topology change. The valid range is 10–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.

- **second-wait milliseconds**
  Specifies the minimum number of milliseconds to wait between the first and second SPF calculation. The valid range is 1–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.

- **max-wait milliseconds**
  Specifies the maximum number of milliseconds to wait between two consecutive SPF calculations. Enter a value that is the same or greater than the second wait time value. The valid range is 1000–120000 milliseconds.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-wait milliseconds</td>
<td>1000</td>
</tr>
<tr>
<td>initial-wait milliseconds</td>
<td>100</td>
</tr>
<tr>
<td>second-wait milliseconds</td>
<td>300</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- To reset all three of the SPF wait time intervals back to their default values, use the `spb isis spf-wait` command without specifying any parameters.

- Subsequent SPF calculations, if required, are generated at exponentially increasing intervals of the SPF `second-wait` parameter value until the `maximum-wait` parameter value is reached. For example, if the second-wait interval value is set to 1000 milliseconds, then the next SPF calculation is triggered after
2000 milliseconds and the next SPF calculation after that is triggered at 4000 milliseconds, and so on, until the maximum-wait interval value is reached.

- When the maximum interval value is reached, the SPF wait interval will stay at the maximum value until there are no more SPF calculations scheduled during that interval. After a full interval without any SPF calculations, the SPF wait interval will reset back to the initial-wait parameter interval value.

**Examples**
-> spb isis spf-wait max-wait 2500 initial-wait 1000 second-wait 1500
-> spb isis spf-wait max-wait 5000
-> spb isis spf-wait initial-wait 1000
-> spb isis spf-wait second-wait 2000
-> spb isis spf-wait

**Release History**
Release 7.3.1; command was introduced.

**Related Commands**
spb isis lsp-wait Configures the time intervals between the first, second, and subsequent generation of link state PDUs (LSPs).
show spb isis info Displays status and configuration information for the SPB instance.

**MIB Objects**
```plaintext
alcatelIND1IsisSpbProtocolConfig
  alcatelIND1IsisSpbProtocolSpfMaxWait
  alcatelIND1IsisSpbProtocolSpfInitialWait
  alcatelIND1IsisSpbProtocolSpfSecondWait
```
**spb isis lsp-wait**

Configures the time intervals between the first, second and subsequently generated link state PDU (LSP).

`spb isis lsp-wait {max-wait milliseconds | initial-wait milliseconds | second-wait milliseconds}`

### Syntax Definitions

**max-wait milliseconds**

Specifies the maximum number of seconds to wait between two consecutively generated LSPs. Enter a value that is the same or greater than the second wait time value. The valid range is 1000–120000 milliseconds.

**initial-wait milliseconds**

Specifies the number of seconds to wait before triggering an initial LSP generation after a topology change. The valid range is 0–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.

**second-wait milliseconds**

Specifies the minimum number of seconds to wait between the first and second generated LSPs. The valid range is 1000–100000 milliseconds. Specify a value that is the same or less than the maximum wait time value.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-wait milliseconds</td>
<td>1000</td>
</tr>
<tr>
<td>initial-wait milliseconds</td>
<td>0</td>
</tr>
<tr>
<td>second-wait milliseconds</td>
<td>300</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- To reset all three of the LSP wait time intervals back to their default values, use the `spb isis lsp-wait` command without specifying any parameters.

- Subsequent LSP, if required, are generated at exponentially increasing intervals of the LSP `second-wait` parameter value until the `maximum-wait` parameter value is reached. For example, if the second-wait interval value is set to 10 seconds, then the next LSP is generation is triggered after 20 seconds and the next LSP generated after that is triggered at 40 seconds, and so on, until the maximum-wait interval value is reached.
When the maximum interval value is reached, the LSP wait interval will stay at the maximum value until there are no more LSP generations during that interval. After a full interval without any LSP generations, the LSP wait interval will reset back to the initial-wait parameter interval value.

**Examples**

- `spb isis lsp-wait max-wait 2000 initial-wait 1000 second-wait 1500`
- `spb isis lsp-wait max-wait 5000`
- `spb isis lsp-wait initial-wait 2500`
- `spb isis lsp-wait second-wait 3000`
- `spb isis lsp-wait`

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `spb isis spf-wait` Configures the time intervals between the first, second, and subsequent shortest path first (SPF) calculations.
- `show spb isis info` Displays status and configuration information for the SPB instance.

**MIB Objects**

- `alcatelIND1IsisSpbProtocolConfig`
  - `alcatelIND1IsisSpbProtocolLspMaxWait`
  - `alcatelIND1IsisSpbProtocolLspInitialWait`
  - `alcatelIND1IsisSpbProtocolLspSecondWait`
spb isis rapid-lsp-converge

Configures the status of ISIS-SPB rapid link state PDU (LSP) convergence and reserves an SPB I-SID to identify a multicast domain. When rapid LSP convergence is enabled (the default) and a topology event occurs, LSP frames are flooded on the multicast domain to all participating SPB bridges to expedite network notification and convergence time.

**spb isis rapid-lsp-converge {isid instance_id | admin-state {enable | disable}}**

**Syntax Definitions**

- **instance_id**: An SPB service instance identifier (I-SID). The valid range is 256–16777214 (or 0.1.0–255.255.254 in dot-decimal notation format).
- **enable**: Enables rapid LSP convergence.
- **disable**: Disables rapid LSP convergence.

**Defaults**

By default, rapid LSP convergence is enabled for the switch and the I-SID number is set to 16776961 or 255.255.1.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The reserved I-SID is always associated with the control BVLAN and is only modifiable when rapid LSP convergence is disabled.
- When changing the default I-SID value, make sure the new value specified is not associated with any SPB service. The specified I-SID will be reserved only for rapid LSP convergence.

**Examples**

- `-> spb isis rapid-lsp-convergence admin-state disable`
- `-> spb isis rapid-lsp-convergence isid 4001`
- `-> spb isis rapid-lsp-convergence isid 220.1.1`
- `-> spb isis rapid-lsp-convergence admin-state enable`

**Release History**

Release 8.5R2; command was introduced.
Related Commands

show spb isis rapid-lsp-converge-info
Displays the ISIS-SPB rapid LSP convergence information for the switch.

show spb isis rapid-lsp-converge-table
Displays the multicast forwarding information for all of the SPB bridges that are participating in rapid LSP convergence.

MIB Objects

alcatelIND1ISISSpbRapidLspConvergence
  alcatelIND1ISISSpbRapidLspConvergenceAdminStatus
  alcatelIND1ISISSpbRapidLspConvergenceIsid
**spb isis overload**

Configures the LSP database overload state for the local ISIS-SPB switch and optionally specifies the amount of time the switch remains in this state. When the overload state is enabled, the switch signals to other ISIS-SPB switches that it is not able to accept transit traffic.

**spb isis overload [timeout seconds]**

**no spb isis overload**

**Syntax Definitions**

*seconds* Specifies the timeout interval, in seconds. The valid range is 60–1800.

**Defaults**

By default, the IS-IS overload state is disabled.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to make the router exit the overload state.
- If the time period is not specified, the router remains in the overload state for an infinite period.
- During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is used only if the destination route is directly reachable by the router (for example, it will not be used for other transit traffic).
- This command can be used when the router is overloaded or before executing a shutdown command to divert traffic around the router.

**Examples**

- `-> spb isis overload timeout 70`
- `-> no spb isis overload`
**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **spb isis overload-on-boot**
  Configures the ISIS-SPB instance to operate in an overload state during bootup for a specified time period.

- **show spb isis info**
  Displays status and configuration information for the ISIS-SPB instance.

**MIB Objects**

- alcatelIND1IsisSpbSysSetOverload
- alcatelIND1IsisSpbSysOverloadTimeout
- alcatelIND1IsisSpbSysOverloadStatus
**spb isis overload-on-boot**

Configures the ISIS-SPB switch to operate in the overload state after a system bootup for the specified amount of time.

```
spb isis overload-on-boot [timeout seconds]
```

```
no spb isis overload-on-boot
```

**Syntax Definitions**

`seconds` Specifies the timeout interval, in seconds. The valid range is 60–1800.

**Defaults**

By default, the ISIS-SPB switch will not operate in the overload state after a bootup.

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- Use the `no` form of this command to prevent the switch from entering the overload state after bootup.
- This command configures the switch to operate in the overload state after a bootup and until the timeout value expires or the `no` form of this command is used.
- The `no spb isis overload` command does not influence the overload-on-boot function.

**Examples**

```
-> spb isis overload-on-boot timeout 80
-> no spb isis overload-on-boot
```

**Release History**

Release 7.3.1; command was introduced.
**Related Commands**

- `spb isis overload`  
  Sets the ISIS-SPB switch to operate in the overload state.

- `show spb isis info`  
  Displays status and configuration information for the ISIS-SPB instance.

**MIB Objects**

- `vRtrIsisTable`
  - `alcatelIND1IsisSpbSysOverloadOnBoot`
  - `alcatelIND1IsisSpbSysOverloadOnBootTimeout`
  - `alcatelIND1IsisSpbSysOverloadStatus`
**spb isis graceful-restart**

Configures graceful restart of the bridge. It allows ISIS-SPB to reconverge faster, minimizing service interruption.

**spb isis graceful-restart**

**no spb isis graceful-restart**

**Syntax Definitions**

N/A

**Defaults**

By default, the graceful restart functionality is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable graceful restart and remove the graceful restart configuration from the SPB bridge.
- When graceful restart is enabled, the bridge can either be a helper (which helps a neighbor router to restart) or a restarting router, or both.

**Examples**

```
-> spb isis graceful-restart
-> no spb isis graceful-restart
```

**Release History**

Release 7.3.1; command was introduced.
Related Commands

spb isis graceful-restart helper  Configures the helper mode of routers for graceful restart.
show spb isis info  Displays status and configuration information for the SPB instance.

MIB Objects

alcatelIND1IsisSpbProtocolConfig
   alcatelIND1IsisSpbProtocolGracefulRestart
spb isis graceful-restart helper

Administratively enables and disables the ISIS-SPB bridge to operate in the helper mode in response to a bridge performing a graceful restart.

spb isis graceful-restart helper {enable | disable}

Syntax Definitions

enable

   Enables the helper mode on the bridge.

disable

   Disables the helper mode on the bridge.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

When graceful restart is enabled, the helper mode is enabled by default.

Examples

-> spb isis graceful-restart helper disable

Release History

Release 7.3.1; command was introduced.

Related Commands

spb isis graceful-restart

   Configures graceful restart on the bridge.

show spb isis info

   Displays status and configuration information for the SPB instance.

MIB Objects

alcatelIND1IsisSpbProtocolConfig
   alcatelIND1IsisSpbProtocolGRHelperMode
show spb isis info

Displays the global ISIS-SPB status and configuration information for the SPB bridge.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td>X48C6/T48C6/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show spb isis info
SPB ISIS Bridge Info:
    System Id = e8e7.3233.1831,
    System Hostname = BEB-1,
    SPSourceID = 03-18-31,
    SPBM System Mode = auto,
    BridgePriority = 32768 (0x8000),
    MT ID = 0,
    Control BVLAN = 4001,
    Area Address = 0.0.0,
    Level Capability = L1,
    Admin State = UP,
    LSDB Overload = Disabled,
    Last Enabled = Thu Aug 2 22:43:19 2012,
    Last SPF = Fri Aug 3 18:15:51 2012,
    SPF Wait = Max: 1000 ms, Initial: 100 ms, Second: 300 ms,
    LSP Lifetime = 1200,
    LSP Wait = Max: 1000 ms, Initial: 0 ms, Second: 300 ms,
    Graceful Restart = Disabled,
    GR helper-mode = Disabled,
    # of L1 LSPs = 8
    Control Address = 01:80:c2:00:00:14 (AllL1)
**Release History**

- Release 7.3.1; command was introduced.
- Release 7.3.2; **Control Address** field added.
Related Commands

**show spb isis spf**
Displays the shortest path first (SPF) information to all known SPB bridges for a specific BVLAN.

**show spb isis bvlans**
Displays the ISIS-SPB backbone VLAN (BVLAN) configuration for the bridge.

**show spb isis interface**
Displays the ISIS-SPB network interface configuration for the bridge.

MIB Objects

alcatelIND1IsisSpbSys
  alcatelIND1IsisSpbSysSysId
  alcatelIND1IsisSpbSysSysName
  alcatelIND1IsisSpbmSysSysSPSourceId
  alcatelIND1IsisSpbmSysSysMode
  alcatelIND1IsisSpbmSysSysBridgePriority
  alcatelIND1IsisSpbmSysSysControlBvlan
  alcatelIND1IsisSpbmSysSysAreaAddress
  alcatelIND1IsisSpbmSysSysAdminState
  alcatelIND1IsisSpbProtocolSpfMaxWait
  alcatelIND1IsisSpbProtocolSpfInitialWait
  alcatelIND1IsisSpbProtocolSpfSecondWait
  alcatelIND1IsisSpbProtocolLspMaxWait
  alcatelIND1IsisSpbProtocolLspInitialWait
  alcatelIND1IsisSpbProtocolLspSecondWait
  alcatelIND1IsisSpbProtocollGRHelperMode
  alcatelIND1IsisSpbSysSysControlAddr
show spb isis bvlans

Displays the ISIS-SPB backbone VLAN (BVLAN) configuration for the bridge.

show spb isis nodes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command also displays the equal cost tree (ECT) algorithm that is assigned to each BVLAN.

Examples

-> show spb isis bvlans
SPB ISIS BVLANs:

<table>
<thead>
<tr>
<th>BVLAN</th>
<th>ECT-algorithm</th>
<th>In Use</th>
<th>Services Mapped</th>
<th>ISIDS</th>
<th>Tandem</th>
<th>Multicast</th>
<th>Root Bridge (Name : MAC Address)</th>
</tr>
</thead>
<tbody>
<tr>
<td>501</td>
<td>00-80-c2-01</td>
<td>NO</td>
<td>NO</td>
<td>0</td>
<td>GMODE</td>
<td>BRIDGE-3:00:d1:95:00:30:02</td>
<td></td>
</tr>
<tr>
<td>502</td>
<td>00-80-c2-02</td>
<td>NO</td>
<td>NO</td>
<td>0</td>
<td>SGMODE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>503</td>
<td>00-80-c2-03</td>
<td>YES</td>
<td>NO</td>
<td>4</td>
<td>SGMODE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>504</td>
<td>00-80-c2-04</td>
<td>YES</td>
<td>NO</td>
<td>4</td>
<td>SGMODE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

BVLANs: 4

output definitions

<table>
<thead>
<tr>
<th>BVLAN</th>
<th>The VLAN ID number for the SPB BVLAN. Configured through the spb bvlan command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECT-algorithm</td>
<td>The equal cost tree (ECT) algorithm index (1–16) assigned to the BVLAN. Configured through the spb isis bvlan ect-id command.</td>
</tr>
<tr>
<td>In Use</td>
<td>Indicates whether or not the BVLAN is in use.</td>
</tr>
<tr>
<td>Services Mapped</td>
<td>Indicates whether or not any local services are mapped to the BVLAN.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Num ISIDS</td>
<td>The number of services known to the BVLAN.</td>
</tr>
<tr>
<td>Tandem Multicast</td>
<td>The tandem multicast mode (SGMODE or GMODE) for the BVLAN. Configured through the <code>spb isis bvlan tandem-multicast-mode</code> command.</td>
</tr>
<tr>
<td>Root Bridge (Name : MAC Address)</td>
<td>The system name and bridge MAC address of the root bridge. This value is displayed only for GMODE configurations.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

- `show spb isis info` Displays status and configuration information for the SPB instance
- `show spb isis interface` Displays the ISIS-SPB network interface configuration for the bridge.

MIB Objects

N/A
show spb isis interface

Displays the ISIS-SPB network interface configuration for the switch.

show spb isis interface [port chassis/slot/port | linkagg agg_id]

Syntax Definitions

chassis/slot/port The chassis, slot, and port number (3/1/1).
agg_id The link aggregate ID number.

Defaults

By default, a list of ISIS-SPB interfaces is displayed with summary information.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command also shows the operational and administrative status of the interface.
- Use the port or linkagg parameter to display additional information for a specific ISIS-SPB interface.
- When an SPB interface is created, the interface is automatically assigned to each SPB BVLAN in the switch configuration.

Examples

-> show spb isis interface

SPB ISIS Interfaces:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Level</th>
<th>CircID</th>
<th>Oper state</th>
<th>Admin state</th>
<th>Link Metric</th>
<th>Hello Intvl</th>
<th>Hello Mult</th>
<th>Hello Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>L1</td>
<td>1</td>
<td>DOWN</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
<tr>
<td>1/1/2</td>
<td>L1</td>
<td>2</td>
<td>UP</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
<tr>
<td>1/1/3</td>
<td>L1</td>
<td>3</td>
<td>DOWN</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
<tr>
<td>1/1/4</td>
<td>L1</td>
<td>4</td>
<td>DOWN</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
<tr>
<td>1/1/5</td>
<td>L1</td>
<td>5</td>
<td>UP</td>
<td>UP</td>
<td>10</td>
<td>3</td>
<td>3</td>
<td>Multi-Access</td>
</tr>
<tr>
<td>1/1/6</td>
<td>L1</td>
<td>6</td>
<td>DOWN</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
<tr>
<td>1/1/7</td>
<td>L1</td>
<td>7</td>
<td>DOWN</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
<tr>
<td>1/1/10</td>
<td>L1</td>
<td>9</td>
<td>DOWN</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
<tr>
<td>0/3</td>
<td>L1</td>
<td>1</td>
<td>UP</td>
<td>UP</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>Pt-to-Pt</td>
</tr>
</tbody>
</table>

Interfaces : 9
**output definitions**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level</td>
<td>The IS-IS Area Level (L1) for the interface.</td>
</tr>
<tr>
<td>CircID</td>
<td>The circuit ID of the interface.</td>
</tr>
<tr>
<td>Oper-state</td>
<td>The operational state of the interface (UP or DOWN).</td>
</tr>
<tr>
<td>Admin-state</td>
<td>The administrative state of the interface (UP or DOWN).</td>
</tr>
<tr>
<td>Link Metric</td>
<td>The metric value of the router for the corresponding area level.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The number of seconds the interface waits between Hello PDU transmissions.</td>
</tr>
<tr>
<td>Hello Multiplier</td>
<td>The number that is multiplied by the Hello Interval to determine the hold time.</td>
</tr>
<tr>
<td>Circ Type</td>
<td>Indicates whether the interface was configured as a point-to-point (P2P) link or as a multiple access (multi-access) link.</td>
</tr>
</tbody>
</table>

```
-> show spb isis interface port 1/1/5
=============
         Interface     |       Type     |
---------------------|----------------|
        1/1/5           | Multi-Access  |
 Oper State          |           UP   |
 Circuit Id          |             1 |
 Desg IS             | 00d0.9501.44bc|
 Metric              |             10 |
 Hello Mult          |             3  |
 Adjacencies         |             3  |
 CSNP Int            |          10 sec|
 Hello Timer         |             3 sec|
 Priority            |             64 |

-> show spb isis interface linkagg 3
=============
         Interface    |       Type     |
-------------------|----------------|
        0/3           | Pt-to-Pt       |
 Oper State        |           UP   |
 Circuit Id        |             1 |
 Desg IS           | N/A           |
 Metric            |             10 |
 Hello Mult        |             3  |
 Adjacencies       |             1  |
 Hello Timer       |             9 sec|
 Priority          |             64 |
```

**output definitions**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Indicates whether the interface was configured as a point-to-point (P2P) link or as a multiple access (multi-access) link.</td>
</tr>
<tr>
<td>Oper-state</td>
<td>The operational state of the interface (UP or DOWN).</td>
</tr>
<tr>
<td>Admin-state</td>
<td>The administrative state of the interface (UP or DOWN).</td>
</tr>
<tr>
<td>Circuit Id</td>
<td>The circuit ID of the interface.</td>
</tr>
<tr>
<td>CSNP Int</td>
<td>The number of seconds the interface waits between Complete Sequence Number PDUs (CSNP) transmissions.</td>
</tr>
<tr>
<td>Desg IS</td>
<td>Indicates if the multiple access interface is operating as a Designated Intermediate System (DIS). This field displays N/A if the interface is not a DIS.</td>
</tr>
<tr>
<td>Adjacencies</td>
<td>The number of adjacencies associated with this interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric value of the router for the corresponding area level.</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hello Timer</strong></td>
<td>The number of seconds the interface waits between Hello PDU transmissions.</td>
</tr>
<tr>
<td><strong>Hello Mult</strong></td>
<td>The number that is multiplied by the Hello Interval to determine the hold time.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>The priority value assigned to this interface. This value is used to elect a DIS for a multiple access domain configuration and does not apply to point-to-point SPB interfaces.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.
Release 8.7R1; “Circ Type” field added; **port** and **linkagg** parameters added.

**Related Commands**

spb isis interface

Creates an ISIS-SPB network interface.

**MIB Objects**

alcatelIND1IsisSpbAdjStaticTable
  - alcatelIND1IsisSpbAdjStaticEntryIfIndex
  - alcatelIND1IsisSpbAdjStaticEntryMetric
  - alcatelIND1IsisSpbAdjStaticEntryHelloInterval
  - alcatelIND1IsisSpbAdjStaticEntryHelloMultiplier
  - alcatelIND1IsisSpbAdjStaticEntryIfAdminState
  - alcatelIND1IsisSpbAdjStaticEntryIfType
show spb isis adjacency

Displays information about the ISIS-SPB adjacencies created for the SPB bridge.

show spb isis adjacency [detail]

Syntax Definitions

detail Displays additional information about the ISIS-SPB adjacencies.

Defaults

By default, a summary list of adjacency information is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show spb isis adjacency

SPB ISIS Adjacency:

<table>
<thead>
<tr>
<th>System (Name : SystemId)</th>
<th>Type</th>
<th>State</th>
<th>Hold</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge-3</td>
<td>L1</td>
<td>UP</td>
<td>25</td>
<td>0/1</td>
</tr>
<tr>
<td>Bridge-4</td>
<td>L1</td>
<td>UP</td>
<td>18</td>
<td>0/1</td>
</tr>
<tr>
<td>Bridge-5</td>
<td>L1</td>
<td>UP</td>
<td>26</td>
<td>0/1</td>
</tr>
</tbody>
</table>

Adjacencies : 3

output definitions

Name The system name assigned to the adjacent SPB bridge.
SystemId The system ID of the adjacent SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
Type The level (L1) of the adjacent bridge.
State The state of the adjacency (UP or DOWN).
Hold The adjacency hold time, in seconds.
output definitions

<table>
<thead>
<tr>
<th>Interface</th>
<th>The slot/port or link aggregate ID of the SPB interface on which the adjacency was formed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjacencies</td>
<td>The total number of adjacent SPB bridges.</td>
</tr>
</tbody>
</table>

-> show spb isis adjacency detail
SPB ISIS Adjacency detail:

SystemID: 00d0.9506.4c62 :
  B-MAC : 00:d0:95:06:4c:62 , Hostname : bridge3 ,
  Interface : 0/1 , Up Time : Mon Sep 26 17:54:29 2011 ,
  State : UP , Priority : 0 ,
  Hold Time : 18 , Max Hold : 27 ,
  Adj Level : L1 , NLPIDs : SPB ,
  ExtLocalCktId(YES): 2,
  Restart Support : Disabled ,
  Restart Status : Not currently being helped ,
  Restart Supressed : Disabled

SystemID: 00d0.9507.9732 :
  B-MAC : 00:d0:95:07:97:32 , Hostname : bridge4 ,
  Interface : 0/1 , Up Time : Mon Sep 26 17:54:29 2011 ,
  State : UP , Priority : 0 ,
  Hold Time : 21 , Max Hold : 27 ,
  Adj Level : L1 , NLPIDs : SPB ,
  ExtLocalCktId(YES): 2,
  Restart Support : Disabled ,
  Restart Status : Not currently being helped ,
  Restart Supressed : Disabled

SystemID: 00d0.9501.51dc :
  B-MAC : 00:d0:95:01:51:dc , Hostname : bridge5 ,
  Interface : 0/1 , Up Time : Mon Sep 26 17:54:29 2011 ,
  State : UP , Priority : 0 ,
  Hold Time : 21 , Max Hold : 27 ,
  Adj Level : L1 , NLPIDs : SPB ,
  ExtLocalCktId(YES): 2,
  Restart Support : Disabled ,
  Restart Status : Not currently being helped ,
  Restart Supressed : Disabled

Adjacencies : 3

output definitions

<table>
<thead>
<tr>
<th>SystemID</th>
<th>The system ID of the adjacent SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-MAC</td>
<td>The backbone MAC address (system ID) of the adjacent bridge. This is the address that is used as the source address for encapsulated customer traffic that is tunneled through SPB services.</td>
</tr>
<tr>
<td>Interface</td>
<td>The slot/port or link aggregate ID of the SPB interface on which the adjacency was formed.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the adjacency (UP or DOWN).</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The adjacency hold time, in seconds.</td>
</tr>
<tr>
<td>Adj Level</td>
<td>The adjacency level (L1) of the SPB bridge.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>ExtLocalCktId(YES)</th>
<th>The circuit ID that the peer bridge has assigned to this adjacency.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart Support</td>
<td>Indicates if graceful restart is Enabled or Disabled.</td>
</tr>
<tr>
<td>Restart Status</td>
<td>Indicates whether the adjacent SPB bridge is helping the local bridge to restart (Not currently being helped or Currently being helped).</td>
</tr>
<tr>
<td>Restart Suppressed</td>
<td>Indicates whether or not the advertisement of LSPs is suppressed per the request of adjacent SPB bridge (Enabled or Disabled).</td>
</tr>
<tr>
<td>Hostname</td>
<td>The system name assigned to the adjacent SPB bridge.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Indicates the time period in seconds, during which the SPB bridge was in the adjacency.</td>
</tr>
<tr>
<td>Priority</td>
<td>The bridge priority value of the adjacent SPB bridge.</td>
</tr>
<tr>
<td>Max Hold</td>
<td>Indicates the maximum hold time of the adjacent SPB bridge.</td>
</tr>
<tr>
<td>NLPIDs</td>
<td>The Network Layer Protocol ID (NLPID) of the adjacent bridge (SPB NLPID = 0xC1).</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

- **show spb isis database**: Displays ISIS-SPB topology information maintained in the link state database (LSDB).
- **show spb isis nodes**: Displays the discovered node-level parameter values for all of the ISIS-SPB bridges participating in the topology.

MIB Objects

N/A
**show spb isis database**

Displays ISIS-SPB topology information maintained in the link state database (LSDB).

`show ip isis database [lsp-id lsp_id]`

---

**Syntax Definitions**

`lsp_id` The LSP ID.

**Defaults**

By default, the entire LSDB is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `lsp-id` parameter with this command to view database information for a specific link state packet (LSP).

- An additional LSP, referred to as a pseudo-node LSP, is transmitted by the Designated Intermediate Switch (DIS) in an SPB multiple access domain. The pseudo-node LSP contains a list of all SPB nodes.

- If the LSP ID specified is a pseudo-node LSP that is generated by a Designated Intermediate Switch (DIS) in an SPB multiple access domain, the contents displayed will differ from that of a regular LSP generated in a point-to-point domain.
  - A DIS pseudo-node LSP lists all the SPB nodes that are connected to multiple access links as neighbors.
  - A regular LSP lists only the neighboring SPB node adjacency.

**Examples**

```
-> show spb isis database
Legends:  P   = The Partition repair bit is set
          OV  = The overload bit is set
          ATT = The Attach bit is set
          L1  = Specifies a Level 1 IS type
          L2  = Specifies a Level 2 IS type

SPB ISIS LSP Database:
LSP ID    Sequence Checksum  Lifetime Attributes
------------------------+-----------+----------+--------+--------+--------+
00d0.9501.084c.00-00   0x04      0xc7f1        763     L1
00d0.9501.2bec.00-00   0x58e     0xede1       1043    L1
```
### Output Definitions

<table>
<thead>
<tr>
<th><strong>LSP ID</strong></th>
<th>The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sequence</strong></td>
<td>The sequence number of the LSP. The sequence number is a value used to identify old and duplicate LSPs.</td>
</tr>
<tr>
<td><strong>Checksum</strong></td>
<td>The checksum value of the LSP.</td>
</tr>
<tr>
<td><strong>Lifetime</strong></td>
<td>The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the LSDB of all the SPB bridges.</td>
</tr>
<tr>
<td><strong>Attributes</strong></td>
<td>The level capability of the bridge. This implementation of ISIS-SPB only supports Level 1 (L1).</td>
</tr>
<tr>
<td><strong>LSP Count</strong></td>
<td>The number of LSPs in the LSDB.</td>
</tr>
</tbody>
</table>

```- show spb isis database lsp-id e8e7.329a.4b0b.00-00
Legends : P = The Partition repair bit is set
OV = The overload bit is set
ATT = The Attach bit is set
L1 = Specifies a Level 1 IS type
L2 = Specifies a Level 2 IS type
SPB ISIS LSP Database:
```

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>e8e7.329a.4b0b.00-00</th>
<th>Level</th>
<th>L1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence</td>
<td>0x2f6</td>
<td>Checksum</td>
<td>0x5799</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
<td>Pkt Type</td>
<td>18</td>
</tr>
<tr>
<td>Attributes</td>
<td>L1</td>
<td>Max Area</td>
<td>3</td>
</tr>
<tr>
<td>SysID Len</td>
<td>6</td>
<td>Used Len</td>
<td>1398</td>
</tr>
<tr>
<td>Alloc Len</td>
<td>1492</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TLVs:**

- **Area Addresses**
  - Area Address : (01) 00
  - Area Address : (03) 00.00.00

- **Supp Protocols**
  - Protocols : SPB

- **IS-Hostname**
  - Hostname : 0S6860

- **TE IS Neighbors**
  - Neighbor : e8e7.329a.57df SPB Metric 10 Num of Ports 1 Port-Id 0x4(1/4)

- **MT Capability**
  - MT-ID : 0x0

- **SPB INSTANCE**

---

00d0.9501.2bec.01-00  0x58d  0x8fd5  902  L1
00d0.9501.330c.00-00  0x596  0x1060  1014 L1
00d0.9501.330c.02-00  0x588  0xd516  996  L1
00d0.9501.44bc.00-00  0x595  0x5998  600  L1
00d0.9501.6d6c.00-00  0xf59c 0xd32e 1070 L1
00d0.9501.6d6c.01-00  0x58b  0x3008  876  L1
00d0.9501.6d6c.03-00  0x588  0x347f  946  L1
00d0.9501.9a6c.00-00  0x593  0xf523  790  L1
00d0.9501.9a6c.01-00  0x58d  0xec84  925  L1
00d0.9501.9a6c.02-00  0x58a  0xb9de  927  L1
00d0.9501.9a6c.03-00  0x58b  0x41ed  861  L1

Level-1 LSP count : 13
CIST Root-ID: 0x0 0x0
CIST Ext Root Path Cost: 0x00000000  Bridge Priority: 0x8000
SPSourceID: 0x001a4b0b (Auto)  Number of Trees: 16
[# 1] ECT-algo:0x0080c201 baseVid:4000 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
[# 2] ECT-algo:0x0080c202 baseVid:4001 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
[# 3] ECT-algo:0x0080c203 baseVid:4002 spVid:0 usedByISID:1(I-SID) mode:1(SPBM)
[# 4] ECT-algo:0x0080c204 baseVid:4003 spVid:0 usedByISID:0() mode:1(SPBM)
[# 5] ECT-algo:0x0080c205 baseVid:4004 spVid:0 usedByISID:0() mode:1(SPBM)
[# 6] ECT-algo:0x0080c206 baseVid:4005 spVid:0 usedByISID:0() mode:1(SPBM)
[# 7] ECT-algo:0x0080c207 baseVid:4006 spVid:0 usedByISID:0() mode:1(SPBM)
[# 8] ECT-algo:0x0080c208 baseVid:4007 spVid:0 usedByISID:0() mode:1(SPBM)
[# 9] ECT-algo:0x0080c209 baseVid:4008 spVid:0 usedByISID:0() mode:1(SPBM)
[#10]ECT-algo:0x0080c20a baseVid:4009 spVid:0 usedByISID:0() mode:1(SPBM)
[#11]ECT-algo:0x0080c20b baseVid:4010 spVid:0 usedByISID:0() mode:1(SPBM)
[#12]ECT-algo:0x0080c20c baseVid:4011 spVid:0 usedByISID:0() mode:1(SPBM)
[#13]ECT-algo:0x0080c20d baseVid:4012 spVid:0 usedByISID:0() mode:1(SPBM)
[#14]ECT-algo:0x0080c20e baseVid:4013 spVid:0 usedByISID:0() mode:1(SPBM)
[#15]ECT-algo:0x0080c20f baseVid:4014 spVid:0 usedByISID:0() mode:1(SPBM)
[#16]ECT-algo:0x0080c210 baseVid:4015 spVid:0 usedByISID:0() mode:1(SPBM)

MT Capability

MT-ID : 0x0
SPB SVCID-UCAST-ADDR :
B-MAC e8.e7.32.9a.4b.0b Base-VID 4000
   [ISID# 1] 16776961 (T=1/R=1)
   [ISID# 2] 1000 (T=0/R=0)
SPB SVCID-UCAST-ADDR :
B-MAC e8.e7.32.9a.4b.0b Base-VID 4001
   [ISID# 1] 2000 (T=0/R=0)
SPB SVCID-UCAST-ADDR :
B-MAC e8.e7.32.9a.4b.0b Base-VID 4002
   [ISID# 1] 3000 (T=0/R=0)

IP VPN

MT-ID : 0x0  BVID: 4000  ISID: 1000 (T=0/R=0)
GATEWAY:
1.1.1.34
PREFIX:
   1.1.1.32, metric 1
   12.1.1.0/24, metric 1
   13.1.1.0/24, metric 1
   128.251.40.0/24, metric 1
   172.28.4.0/24, metric 1
   34.1.1.0/24, metric 1

IP VPN

MT-ID : 0x0  BVID: 4000  ISID: 1000 (T=0/R=0)
GATEWAY6:
1035:1::1
PREFIX6:
   3021:1:0:26::/64, metric 1
   3021:1:0:27::/64, metric 1
   3021:1:0:28::/64, metric 1

IP VPN

MT-ID : 0x0  BVID: 4000  ISID: 1000 (T=0/R=0)
GATEWAY6:
1036:1::1
PREFIX6:
   3001:1:0:4d::/64, metric 1

IP VPN

MT-ID : 0x0  BVID: 4000  ISID: 1000 (T=0/R=0)
GATEWAY6:
Sample output of a pseudo-node LSP transmitted from a DIS in an SPB multiple access domain:

`-> show spb isis database lsp-id 00d0.9501.6d6c.01-00`

Legends:
- **P** = The Partition repair bit is set
- **OV** = The overload bit is set
- **ATT** = The Attach bit is set
- **L1** = Specifies a Level 1 IS type
- **L2** = Specifies a Level 2 IS type

SPB ISIS LSP Database:

```
LSP ID        : 00d0.9501.6d6c.01-00                   Level     : L1
Sequence      : 0x58b            Checksum  : 0x3008    Lifetime  : 609
Version       : 1                Pkt Type  : 18        Pkt Ver   : 1
Attributes    : L1               Max Area  : 3
SysID Len     : 6                Used Len  : 105       Alloc Len : 105
```

TLVs:
- TE IS Neighbors:
  - Neighbor : 00d0.9501.6d6c SPB Metric 10 Num of Ports 1 Port-Id 0x104
  - Neighbor : 00d0.9501.330c SPB Metric 10 Num of Ports 1 Port-Id 0x104
  - Neighbor : 00d0.9501.44bc SPB Metric 10 Num of Ports 1 Port-Id 0x104
  - Neighbor : 00d0.9501.20cc SPB Metric 10 Num of Ports 1 Port-Id 0x104

Sample output of an LSP that displays the learned SPB management (SPB-MGMT) routes under the TLV list heading “IPv4 Reach Routes”:

`-> show spb isis database lsp-id 00d0.9501.084c.00-00`

Legends:
- **P** = The Partition repair bit is set
- **OV** = The overload bit is set
- **ATT** = The Attach bit is set
- **L1** = Specifies a Level 1 IS type
- **L2** = Specifies a Level 2 IS type

SPB ISIS LSP Database:

```
LSP ID        : 00d0.9501.084c.00-00                    Level     : L1
Sequence      : 0x04             Checksum  : 0xc7f1     Lifetime  : 763
Version       : 1                Pkt Type  : 18         Pkt Ver   : 1
Attributes    : L1               Max Area  : 3
SysID Len     : 6                Used Len  : 145       Alloc Len : 1492
```

TLVs:
- Area Addresses:
  - Area Address : (01) 00
  - Area Address : (03) 00.00.00
- Supp Protocols:
  - Protocols : SPB
- IPv4 I/F Addresses:
- IPv4 Address : 100.0.0.1
- IPv4 Reach Routes:
  - SPB-MGMT route : 10.0.0.1/32
SPB-MGMT route : 128.251.0.0/16
IS-Hostname :
Hostname : DUT1
TE IS Neighbors :
Neighbor : 00d0.9501.b89c SPB Metric 10 Num of Ports 1 Port-Id 0x120(1/3/32)
MT Capability :
   MT-ID : 0x0
SPB INSTANCE :
   CIST Root-ID: 0x0 0x0
   CIST Ext Root Path Cost: 0x00000000 Bridge Priority: 0x8000
   SPSourceID: 0x0011084c (Auto) Number of Trees: 2
   [#1 ] ECT-algo:0x0080c201 baseVid: 4001 spVid: 0 usedByISID: 1(I-SID) mode: 1(SPBM)
   [#2 ] ECT-algo:0x0080c202 baseVid: 4002 spVid: 0 usedByISID: 0() mode: 1(SPBM)
MT Capability :
   MT-ID : 0x0
SPB SVCID-UCAST-ADDR :
   B-MAC 00.d0.95.01.08.4c Base-VID 4001
   [ISID# 1] 16776961 (T=1/R=1)

Release History

Release 7.3.1; command was introduced.
Release 8.5R2; display output updated to include SPB IPv6 VPN information.
Release 8.7R1; display output updated to include pseudo-node LSP information.

Related Commands

**show spb isis adjacency**
Displays information about the ISIS-SPB adjacencies created for the SPB bridge.

**show spb isis nodes**
Displays the discovered node-level parameter values for all of the ISIS-SPB bridges participating in the topology.

MIB Objects

N/A
show spb isis nodes

Displays the discovered node-level parameter values for all of the ISIS-SPB switches participating in the topology.

show spb isis nodes

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the system name, system ID, SPsource ID, and bridge priority parameter values for the bridges discovered within the ISIS-SPB topology.

**Examples**

```bash
-> show spb isis nodes
SPB ISIS Nodes:
System Name          System Id      SourceID BridgePriority
--------------------+---------------+--------+---------------
Bridge-1 00e0.b1e7.0188  0x70188  32768 (0x8000)
Bridge-2 00e0.b1e7.0bd3  0x70bd3  32768 (0x8000)
Bridge-4 e8e7.3200.2ald 0x02a1d  32768 (0x8000)
Bridge-5 e8e7.3233.1891 0x31891  32768 (0x8000)
Bridge-6 e8e7.3233.199d 0x3199d  32768 (0x8000)
Bridge-7 e8e7.3233.1a29 0x31a29  32768 (0x8000)
Bridge-8 e8e7.3233.1c81 0x31c81  32768 (0x8000)
```

**output definitions**

- **System Name**
  - The system name assigned to the SPB bridge.

- **System Id**
  - The system ID of the SPB bridge. The system ID is the base chassis MAC address of the SPB bridge.
output definitions (continued)

<table>
<thead>
<tr>
<th>SourceID</th>
<th>The shortest path (SP) source ID value for the SPB bridge. This value identifies the source of multicast frames and is relevant only in the multicast tandem replication mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BridgePriority</td>
<td>The bridge priority value assigned to the SPB bridge.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **show spb isis adjacency** Displays information about the ISIS-SPB adjacencies created for the SPB bridge.
- **show spb isis info** Displays status and configuration information for the SPB instance

**MIB Objects**

N/A
**show spb isis unicast-table**

Displays the unicast forwarding information for the specified BVLANs. Use this command to verify unicast addresses were learned correctly on each SPB switch in the ISIS-SPB backbone topology.

**show spb isis unicast-table [bvlan bvlan_id]**

---

**Syntax Definitions**

**bvlan_id**

The VLAND ID of an existing BVLAN.

---

**Defaults**

By default, the forwarding information for all BVLANs in the SPB topology is displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the **bvlan bvlan_id** parameter to display information for a specific BVLAN.

---

**Examples**

```bash
-> show spb isis unicast-table
SPB ISIS Unicast MAC Table:

<table>
<thead>
<tr>
<th>BVLAN (Name : MAC Address)</th>
<th>Outbound Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>4001 BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>1/1</td>
</tr>
<tr>
<td>4001 BRIDGE-4 : e8:e7:32:00:2a:1d</td>
<td>1/1</td>
</tr>
<tr>
<td>4001 BRIDGE-5 : e8:e7:32:33:18:91</td>
<td>1/3</td>
</tr>
<tr>
<td>4001 BRIDGE-6 : e8:e7:32:33:19:9d</td>
<td>1/1</td>
</tr>
<tr>
<td>4001 BRIDGE-7 : e8:e7:32:33:1a:29</td>
<td>1/2</td>
</tr>
<tr>
<td>4001 BRIDGE-8 : e8:e7:32:33:1c:81</td>
<td>1/1</td>
</tr>
<tr>
<td>4002 BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>1/1</td>
</tr>
<tr>
<td>4002 BRIDGE-4 : e8:e7:32:00:2a:1d</td>
<td>1/3</td>
</tr>
<tr>
<td>4002 BRIDGE-5 : e8:e7:32:33:18:91</td>
<td>1/3</td>
</tr>
<tr>
<td>4002 BRIDGE-6 : e8:e7:32:33:19:9d</td>
<td>1/2</td>
</tr>
<tr>
<td>4002 BRIDGE-7 : e8:e7:32:33:1a:29</td>
<td>1/2</td>
</tr>
<tr>
<td>4002 BRIDGE-8 : e8:e7:32:33:1c:81</td>
<td>1/3</td>
</tr>
<tr>
<td>4003 BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>1/1</td>
</tr>
<tr>
<td>4003 BRIDGE-4 : e8:e7:32:00:2a:1d</td>
<td>1/3</td>
</tr>
<tr>
<td>4003 BRIDGE-5 : e8:e7:32:33:18:91</td>
<td>1/3</td>
</tr>
<tr>
<td>4003 BRIDGE-6 : e8:e7:32:33:19:9d</td>
<td>1/3</td>
</tr>
<tr>
<td>4003 BRIDGE-7 : e8:e7:32:33:1a:29</td>
<td>1/2</td>
</tr>
</tbody>
</table>
```
4003 BRIDGE-8 : e8:e7:32:33:1c:81 1/3
4004 BRIDGE-2 : 00:e0:b1:e7:0b:d3 1/1
4004 BRIDGE-4 : e8:e7:32:00:2a:1d 1/1
4004 BRIDGE-5 : e8:e7:32:33:18:91 1/3
4004 BRIDGE-6 : e8:e7:32:33:19:9d 1/1
4004 BRIDGE-7 : e8:e7:32:33:1a:29 1/2
4004 BRIDGE-8 : e8:e7:32:33:1c:81 1/1

MAC Addresses: 24

-> show spb isis unicast-table bvlan 4001

<table>
<thead>
<tr>
<th>Destination</th>
<th>Outbound Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVLAN</td>
<td>BMAC</td>
</tr>
<tr>
<td>4001 BRIDGE-2     : 00:e0:b1:e7:0b:d3 1/1</td>
<td></td>
</tr>
<tr>
<td>4001 BRIDGE-4     : e8:e7:32:00:2a:1d 1/1</td>
<td></td>
</tr>
<tr>
<td>4001 BRIDGE-5     : e8:e7:32:33:18:91 1/3</td>
<td></td>
</tr>
<tr>
<td>4001 BRIDGE-6     : e8:e7:32:33:19:9d 1/1</td>
<td></td>
</tr>
<tr>
<td>4001 BRIDGE-7     : e8:e7:32:33:1a:29 1/2</td>
<td></td>
</tr>
<tr>
<td>4001 BRIDGE-8     : e8:e7:32:33:1c:81 1/1</td>
<td></td>
</tr>
</tbody>
</table>

MAC Addresses: 6

output definitions

<table>
<thead>
<tr>
<th>BVLAN</th>
<th>System (Name : BMAC)</th>
<th>Outbound Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The VLAN ID number for the SPB BVLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The system name of the destination SPB bridge, and the destination unicast BMAC address for that bridge.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The interface (port or link aggregate) on which the destination system is reached.</td>
<td></td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

- **show spb isis bvlans**: Displays status and configuration information for the SPB instance.
- **show spb isis multicast-table**: Displays the multicast forwarding information for the specified service instance identifier (I-SID).

MIB Objects

N/A
**show spb isis services**

Displays the service instance identifier (I-SID) mapping for bridges participating in the SPB topology. This command provides a network-wide view of existing services to help verify that SPB services are correctly advertised and learned by ISIS-SPB.

**show spb isis services [isid instance_id | bvlan bvlan_id]**

---

**Syntax Definitions**

- **instance_id**: An existing I-SID number.
- **bvlan_id**: The VLAND ID of an existing BVLAN.

---

**Defaults**

By default, the mapping for all I-SIDs in the SPB topology is displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **isid instance_id** number to display information for a specific service instance.
- Use the **bvlan bvlan_id** parameter to display information for a specific BVLAN.

---

**Examples**

```
-> show spb isis services
Legend: * indicates locally configured ISID
SPB ISIS Services Info:
System     ISID   BVLAN (Name : BMAC)     MCAST (T/R)
------------+-------+----------------------------------------+-----------
*     1000     4001   BRIDGE-1 : 00:e0:b1:e7:01:88
*     1000     4001   BRIDGE-4 : e8:e7:32:00:2a:1d
*     1001     4001   BRIDGE-1 : 00:e0:b1:e7:01:88
*     1001     4001   BRIDGE-4 : e8:e7:32:00:2a:1d
*     1002     4001   BRIDGE-1 : 00:e0:b1:e7:01:88
*     1002     4001   BRIDGE-4 : e8:e7:32:00:2a:1d
*     1003     4001   BRIDGE-1 : 00:e0:b1:e7:01:88
*     1003     4001   BRIDGE-4 : e8:e7:32:00:2a:1d
*     1004     4001   BRIDGE-1 : 00:e0:b1:e7:01:88
*     1004     4001   BRIDGE-4 : e8:e7:32:00:2a:1d
*     1005     4001   BRIDGE-1 : 00:e0:b1:e7:01:88
```

---

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 9-76
* 1005  4001  BRIDGE-4  : e8:e7:32:00:2a:1d
* 1006  4001  BRIDGE-1  : 00:e0:b1:e7:01:88
* 1006  4001  BRIDGE-4  : e8:e7:32:00:2a:1d
* 1007  4001  BRIDGE-1  : 00:e0:b1:e7:01:88
* 1007  4001  BRIDGE-4  : e8:e7:32:00:2a:1d

ISIDs: 16

**output definitions**

<table>
<thead>
<tr>
<th>ISID</th>
<th>The service instance identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVLAN</td>
<td>The VLAN ID number for the SPB BVLAN.</td>
</tr>
<tr>
<td>System (Name : BMAC)</td>
<td>The system name of the SPB bridge from where the I-SID was discovered or configured, and the destination unicast BMAC address to which frames associated with the service instance are sent.</td>
</tr>
<tr>
<td>Multicast (T/R)</td>
<td>Indicates the multicast service requirement for the instance (Transmit, Receive, or both).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

* `show spb isis info` Displays status and configuration information for the SPB instance

**MIB Objects**

N/A
show spb isis spf

Displays the shortest path first (SPF) information to all known SPB bridges for a specific BVLAN.

show spb isis spf bvlan \texttt{bvlan\_id} [\texttt{bmac mac\_address}]

### Syntax Definitions

- **bvlan\_id**
  - The VLAND ID of an existing BVLAN.
- **mac\_address**
  - An SPB bridge BMAC address.

### Defaults

By default, the SPF information for all known BMAC addresses for the specified BVLAN.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the \texttt{bmac mac\_address} parameter to display information for a specific SPB bridge.

### Examples

- `-> show spb isis spf bvlan 4001`

  SPB ISIS Path Table:

<table>
<thead>
<tr>
<th>Destination (Name : BMAC)</th>
<th>Outbound Interface (Name : BMAC)</th>
<th>Next Hop BMAC</th>
<th>SPB Metric</th>
<th>Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRIDGE-1 : 00:e0:b1:e7:01:88</td>
<td>1/3</td>
<td>BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>20</td>
<td>2</td>
</tr>
<tr>
<td>BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>1/3</td>
<td>BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>BRIDGE-4 : e8:e7:32:00:2a:1d</td>
<td>1/2</td>
<td>BRIDGE-4 : e8:e7:32:00:2a:1d</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>BRIDGE-6 : e8:e7:32:33:19:9d</td>
<td>1/3</td>
<td>BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>20</td>
<td>2</td>
</tr>
<tr>
<td>BRIDGE-7 : e8:e7:32:33:1a:29</td>
<td>1/3</td>
<td>BRIDGE-2 : 00:e0:b1:e7:0b:d3</td>
<td>30</td>
<td>3</td>
</tr>
</tbody>
</table>

  SPF Path count: 6

- `-> show spb isis spf bvlan 4001 bmac e8:e7:32:33:1a:29`

  SPB ISIS Path Details:

<table>
<thead>
<tr>
<th>Path Hop Name</th>
<th>Path Hop BMAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>BRIDGE-7</td>
<td>e8:e7:32:33:1a:29</td>
</tr>
<tr>
<td>BRIDGE-1</td>
<td>00:e0:b1:e7:01:88</td>
</tr>
<tr>
<td>BRIDGE-2</td>
<td>00:e0:b1:e7:0b:d3</td>
</tr>
</tbody>
</table>
Output Definitions

<table>
<thead>
<tr>
<th>Destination (Name : BMAC)</th>
<th>The system name of the destination SPB bridge, and the destination BMAC address for that bridge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Interface</td>
<td>The interface (port or link aggregate) on which the destination system is reached.</td>
</tr>
<tr>
<td>Next Hop (Name : BMAC)</td>
<td>The system name of the next-hop SPB bridge, and the BMAC address for that bridge.</td>
</tr>
<tr>
<td>SPB Metric</td>
<td>The metric (cost) to reach the destination BMAC address.</td>
</tr>
<tr>
<td>Num Hops</td>
<td>The number of hops along the path to the destination.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

- `show spb isis multicast-sources-spf` Displays the SPF reachability for a known multicast source bridge for a specific BVLAN.
- `show spb isis info` Displays status and configuration information for the SPB instance

MIB Objects

- N/A
show spb isis multicast-table

Displays the multicast forwarding information for the specified service instance identifier (I-SID).

show spb isis multicast-table [isid instance_id]

Syntax Definitions

instance_id An existing I-SID number.

Defaults

By default, the forwarding information for all services in the SPB topology is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the isid instance_id parameter to display information for a specific service instance.

Examples

-> show spb isis multicast-table
SPB ISIS Multicast MAC Table:

<table>
<thead>
<tr>
<th>ISID</th>
<th>BVLAN</th>
<th>MCAST Group Address</th>
<th>MCAST Source</th>
<th>Inbound Interface</th>
<th>Outbound Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td>41</td>
<td>0a:fd:c2:00:01:22</td>
<td>BRIDGE-8</td>
<td>0:0:d0:95:0a:fd:c2</td>
<td>1/2</td>
</tr>
</tbody>
</table>

MAC Addresses: 1

output definitions

<table>
<thead>
<tr>
<th>ISID</th>
<th>The service instance identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVLAN</td>
<td>The VLAN ID number for the SPB BVLAN associated with the service instance.</td>
</tr>
<tr>
<td>MCAST Group Address</td>
<td>The multicast destination group address.</td>
</tr>
<tr>
<td>MCAST Source (Name : BMAC)</td>
<td>The system name and BMAC address of the multicast source.</td>
</tr>
<tr>
<td>Inbound Interface</td>
<td>The interface (port or link aggregate) on which multicast traffic is received for the service instance.</td>
</tr>
<tr>
<td>Outbound Interface</td>
<td>The interface (port or link aggregate) on which multicast traffic is sent for the service instance.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **show spb isis multicast-sources**
  Displays all the known multicast sources across the SPB domain and BVLANs.

- **show spb isis multicast-sources-spf**
  Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

**MIB Objects**

N/A
**show spb isis multicast-sources**

Displays all the known multicast sources across the SPB domain and BVLANs.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command also displays whether or not the source is reachable.

**Examples**

```
-> show spb isis multicast-sources
SPB ISIS Multicast Source Nodes:
  Multicast Source (Name : BMAC)       Reachable  (# ) BVIDS
  -----------------------------------+-------------------  +---------------+----+
  BRIDGE-8 : 00:d0:95:0a:fd:c2       YES         (2)  4001 4002

Total SPB Multicast Source Nodes: 1
```

**output definitions**

- **Multicast Source (Name : BMAC)**: The system name and BMAC address of the multicast source bridge.
- **Reachable**: Indicates whether the multicast source node is reachable (YES or NO).
- **(# ) BVIDS**: Indicates the number of BVLANs and the BVLAN IDs on which the bridge acts as a multicast source.

**Release History**

Release 7.3.1; command was introduced.
### Related Commands

- **show spb isis multicast-sources-spf**
  Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

- **show spb isis multicast-table**
  Displays the multicast forwarding information for the specified service instance identifier (I-SID).

- **show spb isis info**
  Displays status and configuration information for the SPB instance

### MIB Objects

N/A
**show spb isis multicast-sources-spf**

Displays the shortest path first (SPF) reachability for a known multicast source bridge for a specific BVLAN.

**show spb isis multicast-sources-spf bvlan bvlan_id bmac mac_address [dest mac_address]**

---

### Syntax Definitions

- **bvlan_id**
  The VLAN ID of an existing BVLAN.
- **mac_address**
  An SPB bridge BMAC address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **dest mac_address** parameter to display information for a specific SPB bridge.

### Examples

```bash
-> show spb isis multicast-sources-spf bvlan 4001 bmac 00:d0:95:0a:fd:c2
SPB ISIS Path Table:
Destination (Name : BMAC)                      Outbound Interface (Name : BMAC) Next Hop SPB Num Metric Hops
----------------------------------------------------------+-------------------------------+-----------------------------+-----+----+-----+
BRIDGE-1 : 00:d0:95:03:19:12                   1/1  BRIDGE-7 : 00:d0:95:09:79:02      30   3
BRIDGE-2 : 00:d0:95:06:4c:62                   1/1  BRIDGE-7 : 00:d0:95:09:79:02      20   2
BRIDGE-3 : 00:d0:95:07:97:32                   1/1  BRIDGE-7 : 00:d0:95:09:79:02      20   2
BRIDGE-6 : 00:d0:95:08:f2:12                   1/2  BRIDGE-6 : 00:d0:95:08:f2:12      10   1
BRIDGE-7 : 00:d0:95:09:79:02                   1/1  BRIDGE-7 : 00:d0:95:09:79:02      10   1

SPF Path count: 5
```

```bash
-> show spb isis spf bvlan 4001 bmac 00:d0:95:0a:fd:c2 dest 00:d0:95:03:19:12
SPB ISIS Multicast Source Path Details:
Path Hop Name Path Hop BMAC
----------------------------------------
BRIDGE-1 00:d0:95:03:19:12
BRIDGE-3 00:d0:95:07:97:32
BRIDGE-7 00:d0:95:09:79:02
```
**output definitions**

<table>
<thead>
<tr>
<th>Destination (Name : BMAC)</th>
<th>The system name and BMAC address of the destination SPB bridge.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound Interface</td>
<td>The interface (port or link aggregate) on which the destination system is reached.</td>
</tr>
<tr>
<td>Next Hop (Name : BMAC)</td>
<td>The system name and BMAC address of the next-hop SPB bridge.</td>
</tr>
<tr>
<td>SPB Metric</td>
<td>The metric (cost) to reach the destination BMAC address.</td>
</tr>
<tr>
<td>Num Hops</td>
<td>The number of hops along the path to the destination.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show spb isis multicast-sources` Displays all the known multicast sources across the SPB domain and BVLANs.
- `show spb isis multicast-table` Displays the multicast forwarding information for the specified service instance identifier (I-SID).
- `show spb isis spf` Displays the SPF information to all known SPB bridges for a specific BVLAN.
- `show spb isis info` Displays status and configuration information for the SPB instance

**MIB Objects**

N/A
### show spb isis ingress-mac-filter

Displays the ingress MAC filter for multicast traffic for a given BVLAN operating in the (*,G) mode.

```plaintext
show spb isis ingress-mac-filter [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2] | bvlan bvlan_id | bmac mac_address]
```

#### Syntax Definitions

- `chassis`  
  The chassis identifier.

- `slot/port[-port2]`  
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- `agg_id[-agg_id2]`  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- `bvlan_id`  
  The VLAND ID of an existing BVLAN.

- `mac_address`  
  The source MAC address of the multicast traffic allowed on the specified BVLAN and physical port.

#### Defaults

N/A

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>6900 X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- Use the optional command parameters to display specific information with this command.
- Each of the optional command parameters can be combined with any of the other optional parameters within the same command line.

#### Examples

```plaintext
-> show spb isis ingress-mac-filter
SPB ISIS Ingress MAC Table (for GMODE bvlans only):
   Inbound   Multicast source MAC
   BVLAN   Interface  (Name : MAC Address)
-----------------------------------------------
   40   1/1   BRIDGE-1        : 00:d0:95:04:8d:92
MAC Addresses: 1
```
output definitions

<table>
<thead>
<tr>
<th>BVLAN</th>
<th>The VLAN ID number for the SPB BVLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound Interface</td>
<td>The interface (port or link aggregate) on which the multicast source MAC was received.</td>
</tr>
<tr>
<td>System (Name : BMAC)</td>
<td>The system name and MAC address of the multicast traffic source.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show spb isis info` Displays status and configuration information for the SPB instance

**MIB Objects**

- N/A
show spb isis rapid-lsp-converge-info

Displays the status of ISIS-SPB rapid LSP convergence for the SPB bridge.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show spb isis rapid-lsp-converge-info
SPB ISIS Rapid Lsp Converge Info:
  Status = DOWN,
  Control ISID = 255.255.1(0xffff01)

output definitions

Status
  The status of the ISIS-SPB rapid LSP convergence for the bridge (Up or Down).

Control ISID
  The SPB I-SID number that is reserved for rapid LSP convergence.

Release History

Release 8.5R2; command was introduced.
Related Commands

spb isis rapid-lsp-converge  Configures the status of ISIS-SPB rapid LSP convergence.
show spb isis rapid-lsp-converge-table  Displays the multicast forwarding information for all of the SPB bridges that are participating in rapid LSP convergence.

MIB Objects

alcatelIND1IsisSpbRapidLspConvergence
  alcatelIND1IsisSpbRapidLspConvergenceAdminState
  alcatelIND1IsisSpbRapidLspConvergenceIsid
show spb isis rapid-lsp-converge-table

Displays the multicast forwarding information for all the SPB bridges that are participating in rapid LSP convergence.

show spb isis rapid-lsp-converge-table

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show spb isis rapid-lsp-converge-table
SPB ISIS Multicast MAC Table:

<table>
<thead>
<tr>
<th>ISID</th>
<th>BVLAN</th>
<th>MCAST Group Address</th>
<th>MCAST Source (Name: BMAC)</th>
<th>Inbound Interface</th>
<th>Outbound Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>255.255.1</td>
<td>4000</td>
<td>43:d2:72:ff:ff:01</td>
<td>BEB_29_2 :e8:e7:32:e4:d2:72</td>
<td>1/6/14</td>
<td></td>
</tr>
<tr>
<td>255.255.1</td>
<td>4000</td>
<td>53:08:04:ff:ff:01</td>
<td>BEB_25_8 :e8:e7:32:8c:36:0d</td>
<td>1/6/14</td>
<td></td>
</tr>
<tr>
<td>255.255.1</td>
<td>4000</td>
<td>d3:d9:00:ff:ff:01</td>
<td>BEB_25_7 :e8:e7:32:7d:d9:00</td>
<td>1/6/14</td>
<td></td>
</tr>
</tbody>
</table>

MAC Addresses: 3

output definitions

<table>
<thead>
<tr>
<th>ISID</th>
<th>The service instance identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BVLAN</td>
<td>The VLAN ID number for the SPB BVLAN associated with the service instance.</td>
</tr>
<tr>
<td>MCAST Group Address</td>
<td>The multicast destination group address.</td>
</tr>
<tr>
<td>MCAST Source (Name : BMAC)</td>
<td>The system name and BMAC address of the multicast source.</td>
</tr>
</tbody>
</table>
Release History

Release 8.5R2; command was introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spb isis rapid-lsp-converge</td>
<td>Configures the status of ISIS-SPB rapid LSP convergence.</td>
</tr>
<tr>
<td>show spb isis rapid-lsp-converge-info</td>
<td>Displays the status of ISIS-SPB rapid LSP convergence for the SPB bridge.</td>
</tr>
</tbody>
</table>

MIB Objects

N/A
The OmniSwitch supports the following service types:

- **Shortest Path Bridging MAC (SPBM), as defined in the IEEE 802.1aq standard.** The SPBM network topology consists of two layers: the backbone infrastructure (control plane) layer and the services (data plane) layer. ISIS-SPB builds the backbone layer by defining loop-free paths through the backbone network. The service layer is based on the PBB framework as defined in the IEEE 802.1ah standard. SPBM supports the MAC-in-MAC method for data encapsulation. An SPBM service transports the encapsulated traffic over the ISIS-SPB infrastructure.

- **Virtual eXtensible LAN (VXLAN), as defined in the IETF “VXLAN: A Framework for Overlaying Layer 2 Virtualized Networks over Layer 3 Networks” standard.** VXLAN is a Layer 2 overlay network that is used to segment and tunnel device traffic. The backbone (control plane) layer is built through a flooding and learning process. A VXLAN service transports encapsulated traffic through the network. This allows Layer 2 communication between local and remote devices over a Layer 3 network.

- **Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel.** Similar to the OmniSwitch VXLAN implementation, L2 GRE provides a Layer 2 overlay network that is used to isolate and tunnel device traffic between tunnel end points over the underlying IP network.
  - L2 GRE assumes that the tunnel end points (IP addresses) are reachable for tunneling traffic; configuring static routes or routing protocols (such as RIP or OSPF) to ensure end point reachability is required. The BFD protocol can be used to learn the ARP of the next-hop gateway.
  - On switches that will operate as a tunnel aggregation switch, L2 GRE services and associated service objects are configured through Service Manager commands to create multiple tunnel end points.
  - On switches that will operate as a tunnel access switch, a single tunnel end point is created by configuring a UNP profile that defines L2 GRE service parameters. When qualifying traffic is assigned to the profile, the necessary L2 GRE service objects are dynamically created. See Chapter 40, “Access Guardian Commands,” for information about how to configure an L2 GRE UNP profile.

The OmniSwitch Service Manager application provides the ability to configure and manage a service-based architecture consisting of the following logical entities that are required to provision a service:

- **Access Port**—A port or link aggregate configured as a service access port. This type of port defines the point at which traffic from other provider networks or traffic directly from customer networks enters the network infrastructure. The access port is also associated with a Layer 2 profile that specifies how to process protocol control frames received on the port.

- **SPBM, VXLAN, or L2 GRE Service**—A flooding domain for network traffic. A service defines a Virtual Forwarding Instance (VFI) that is capable of learning device MAC addresses from the access side and from the network side and then switching the traffic based on this information.

- **Service Access Point (SAP)**—A SAP is a logical service entity (also referred to as a virtual port) that binds an access port to an SPB service ID, a VXLAN service ID, or an L2 GRE service ID and
specifies the type of customer traffic (untagged, single-tagged, double-tagged, or all) to encapsulate and tunnel through the network infrastructure.

- **Service Distribution Point (SDP)**—An SDP provides a logical point at which customer traffic is directed from one backbone edge switch to another. SDPs are used to set up distributed services, which consist of at least one SAP on a local node, one SAP on a remote node, and an SDP binding the service on both nodes.

- **Bind-SDP**—Represents the binding of a service instance to an SDP. The SDP then distributes the service connectivity to other backbone edge switches.

- **Service Instance Identifier (I-SID)**—An SPB backbone service instance that will tunnel the encapsulated data traffic through the network infrastructure. The I-SID is bound to an SPB backbone VLAN (BVLAN) ID and a Service Manager SPB service ID when the service is created.

- **Virtual Network Identifier (VNID)**—The VNID is a 24-bit segment ID (also referred to as a VXLAN segment ID) that is used to identify encapsulated VM frames. A VNID is bound to a Service Manager VXLAN service ID when the service is created.

- **Virtual Private Network ID (VPNID)**—An L2 GRE tunnel ID that identifies a segment of a tunnel service and is used in the GRE encapsulation header. A VPNID is bound to a Service Manager L2 GRE service ID when the service is created.

This chapter documents the Command Line Interface (CLI) commands used to configure and verify the service-based architecture. For commands used to configure and verify the ISIS-SPB backbone, see Chapter 9, “Shortest Path Bridging Commands.”

MIB information for the Service Manager commands is as follows:

- **Filename:** ALCATEL-IND1-SERVICE-MGR-MIB.mib
- **Module:** alcatelIND1ServiceMgrMIB
A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>Service Commands</th>
<th>Service Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>service spb</td>
<td>service spb</td>
</tr>
<tr>
<td>service pseudo-wire</td>
<td>service pseudo-wire</td>
</tr>
<tr>
<td>service vxlan</td>
<td>service vxlan</td>
</tr>
<tr>
<td>service 12gre</td>
<td>service 12gre</td>
</tr>
<tr>
<td>service description</td>
<td>service description</td>
</tr>
<tr>
<td>service multicast-mode</td>
<td>service multicast-mode</td>
</tr>
<tr>
<td>service stats</td>
<td>service stats</td>
</tr>
<tr>
<td>service vlan-xlation</td>
<td>service vlan-xlation</td>
</tr>
<tr>
<td>service admin-state</td>
<td>service admin-state</td>
</tr>
<tr>
<td>service remove-ingress-tag</td>
<td>service remove-ingress-tag</td>
</tr>
<tr>
<td>service vxlan udp-port</td>
<td>service vxlan udp-port</td>
</tr>
<tr>
<td>service vxlan vrf</td>
<td>service vxlan vrf</td>
</tr>
<tr>
<td>service local-rrp</td>
<td>service local-rrp</td>
</tr>
<tr>
<td>service 12gre reserved-vlan</td>
<td>service 12gre reserved-vlan</td>
</tr>
<tr>
<td>service 13vpn profile</td>
<td>service 13vpn profile</td>
</tr>
<tr>
<td>show service</td>
<td>show service</td>
</tr>
<tr>
<td>show service ports</td>
<td>show service ports</td>
</tr>
<tr>
<td>show service spb sap</td>
<td>show service spb sap</td>
</tr>
<tr>
<td>show service debug-info</td>
<td>show service debug-info</td>
</tr>
<tr>
<td>show service info</td>
<td>show service info</td>
</tr>
<tr>
<td>show service 13vpn profile</td>
<td>show service 13vpn profile</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Access Port Commands</th>
<th>Service Access Port Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>service l2profile</td>
<td>service l2profile</td>
</tr>
<tr>
<td>service l2profile inbound 802.1ab</td>
<td>service l2profile inbound 802.1ab</td>
</tr>
<tr>
<td>service access</td>
<td>service access</td>
</tr>
<tr>
<td>service access l2profile</td>
<td>service access l2profile</td>
</tr>
<tr>
<td>service access vlan-xlation</td>
<td>service access vlan-xlation</td>
</tr>
<tr>
<td>show service l2profile</td>
<td>show service l2profile</td>
</tr>
<tr>
<td>show service access</td>
<td>show service access</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Access Point (SAP) Commands</th>
<th>Service Access Point (SAP) Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>service sap</td>
<td>service sap</td>
</tr>
<tr>
<td>service sap description</td>
<td>service sap description</td>
</tr>
<tr>
<td>service sap trusted</td>
<td>service sap trusted</td>
</tr>
<tr>
<td>service sap stats</td>
<td>service sap stats</td>
</tr>
<tr>
<td>service sap admin-state</td>
<td>service sap admin-state</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service Distribution Point (SDP) Commands</th>
<th>Service Distribution Point (SDP) Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>service sdp vxlan</td>
<td>service sdp vxlan</td>
</tr>
<tr>
<td>service sdp 12gre</td>
<td>service sdp 12gre</td>
</tr>
<tr>
<td>service bind-sdp</td>
<td>service bind-sdp</td>
</tr>
<tr>
<td>service 12gre auto-discover</td>
<td>service 12gre auto-discover</td>
</tr>
<tr>
<td>show service sdp</td>
<td>show service sdp</td>
</tr>
<tr>
<td>show service sdp spb</td>
<td>show service sdp spb</td>
</tr>
<tr>
<td>show service sdp vxlan</td>
<td>show service sdp vxlan</td>
</tr>
<tr>
<td>show service sdp 12gre</td>
<td>show service sdp 12gre</td>
</tr>
<tr>
<td>show service bind-sdp</td>
<td>show service bind-sdp</td>
</tr>
<tr>
<td>show service bind-sdp spb</td>
<td>show service bind-sdp spb</td>
</tr>
<tr>
<td>show service bind-sdp vxlan</td>
<td>show service bind-sdp vxlan</td>
</tr>
<tr>
<td>show service bind-sdp 12gre</td>
<td>show service bind-sdp 12gre</td>
</tr>
<tr>
<td>show service mesh-sdp</td>
<td>show service mesh-sdp</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Statistics Commands</th>
<th>Statistics Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear service counters</td>
<td>clear service counters</td>
</tr>
<tr>
<td>show service counters</td>
<td>show service counters</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote Fault Propagation (RFP)</th>
<th>Remote Fault Propagation (RFP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>service rfp local-endpoint</td>
<td>service rfp local-endpoint</td>
</tr>
<tr>
<td>service rfp remote-endpoint</td>
<td>service rfp remote-endpoint</td>
</tr>
<tr>
<td>show service rfp</td>
<td>show service rfp</td>
</tr>
<tr>
<td>show service rfp configuration</td>
<td>show service rfp configuration</td>
</tr>
</tbody>
</table>
service spb

Configures a Shortest Path Bridging (SPB) service and associates that service with a backbone service instance identifier (I-SID) and BVLAN. An SPB service connects multiple customer sites together across a provider-managed core network by creating a virtual zero-hop, Layer 2 switched domain.

This section describes the base command along with the other optional command keywords that are used to configure SPB service parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a no form to remove the parameter or return it to its default value.

```
service service_id[-service_id2] spb isid instance_id[-instance_id2] bvlan bvlan_id[:x]
  [pseudo-wire {enable | disable}]
  [description desc_info]
  [multicast-mode {head-end | tandem | hybrid}]
  [stats {enable | disable}]
  [vlan-xlation {enable | disable}]
  [admin-state {enable | disable}]

no service service_id spb
```

**Syntax Definitions**

- `service_id[-service_id2]` A unique numerical value to identify a specific SPB service. The valid service ID range is 1–32767. Use a hyphen to configure a range of SPB service IDs (10-13).
- `instance_id[-instance_id2]` A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network. The valid range is 256–16777214. Use a hyphen to configure a range of I-SIDs (300-303).
- `bvlan_id[:x]` The VLAN ID number of an existing SPB BVLAN. To specify a range of BVLANs to assign to a range of services, append the “:x” syntax, where “x” is the number of BVLANs to assign in sequence (for example, 4000:4 would assign BVLANs 4000, 4001, 4002, and 4003).

**Defaults**

When an SPB service is created without specifying any of the optional parameter values, the service is created with the following default values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>pseudo-wire {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>description desc_info</td>
<td>no description added</td>
</tr>
<tr>
<td>tandem</td>
<td>head-end</td>
</tr>
<tr>
<td>stats {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>vlan-xlation {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>admin-state {enable</td>
<td>disable}</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platforms</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860N</th>
<th>6860</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- To remove an SPB service, administratively disable the service (including any associated SAPs and SDPs) then use the `no` form of this command and specify the service ID of the disabled service.

- SPB services created with this command are considered static services, which are identified by a service ID number between 1 and 32767 (the valid range for this command). If the SPB service was dynamically created by another OmniSwitch feature, such as Universal Network Profiles (UNP), a service ID number between 32768 and 65534 is automatically assigned to the dynamic service.

- An SPB service provides E-LAN connectivity for customer traffic and is identified by an I-SID. Services are bound to service access ports (SAPs) on the access side. On the network side they are automatically bound to service distribution points by the ISIS-SPB protocol.

- Each SPB service is basically a Virtual Forwarding Instance (VFI) that is capable of learning customer MAC addresses from the access side (SAPs) and from the network side (Mesh SDP) and then switching the traffic based on this information.

- Use the `pseudo-wire` option to configure the SPB service to provide point-to-point E-LINE connectivity instead of multipoint-to-multipoint E-LAN connectivity. See the `service pseudo-wire` command on page page 10-7 for more information.

Examples

- `service 100 spb isid 1000 bvlan 4001`
- `service 200 spb isid 2000 bvlan 4001 vlan-xlation enable multicast-mode head-end description "SPB service for ISID 2000 in head-end mode"`
- `service 1-100 spb isid 1000-1100 bvlan 4000:4 multicast-mode tandem description "100 SPB Services with ISIDs from 1000-1100 and BVLANs from 4000-4003"`
- `no service 100 spb`

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for specifying a range of IDs, ISIDs, and BVLANs added.
Release 8.7R2; `pseudo-wire` parameter added.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service pseudo-wire</code></td>
<td>Configures an SPB service to operate as a point-to-point (E-LINE) service.</td>
</tr>
<tr>
<td><code>service description</code></td>
<td>Modifies the description information for the service.</td>
</tr>
<tr>
<td><code>service multicast-mode</code></td>
<td>Modifies the multicast replication mode for the service.</td>
</tr>
<tr>
<td><code>service stats</code></td>
<td>Modifies the status of statistics collection for the service.</td>
</tr>
<tr>
<td><code>service vlan-xlation</code></td>
<td>Modifies the status of VLAN translation for the service.</td>
</tr>
<tr>
<td><code>service admin-state</code></td>
<td>Modifies the administrative status for the service.</td>
</tr>
<tr>
<td><code>show service</code></td>
<td>Displays the service configuration for the bridge.</td>
</tr>
</tbody>
</table>

MIB Objects

alaSvcBaseInfoTable
  - alaSvcId
  - alaSvcType
  - alaSvcDescription
  - alaSvcAdminStatus
  - alaSvcStatsAdminStatus
  - alaSvcIsid
  - alaSvcBVlan
  - alaSvcMulticastMode
  - alaSvcSapVlanXlation
  - alaSvcOption
**service pseudo-wire**

Configures the specified Shortest Path Bridging (SPB) service to operate as a point-to-point (E-LINE) service.

```
service service_id pseudo-wire {enable | disable}
```

**Syntax Definitions**

- **service_id**: An SPB service ID number.
- **pseudo-wire enable**: The SPB service will operate as a point-to-point (E-LINE) service. MAC address learning for the service is automatically turned off.
- **pseudo-wire disable**: The SPB service will operate as a multipoint-to-multipoint (E-LAN) service (the default). MAC addresses for the service are learned.

**Defaults**

By default, an SPB service provides multipoint-to-multipoint (E-LAN) connectivity between customer sites across an SPB network.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **disable** option to revert the SPB service back to operating in the default mode (multipoint-to-multipoint).
- With a pseudo-wire point-to-point connection, there is no forwarding decision to be made; packets simply enter one end of the connection and leave the other end of the connection unchanged. As a result, customer MAC addresses are not learned on the SAP attachment points. Packets are transparently forwarded, which simplifies traffic flow and reduces hardware usage.
- An SPB pseudo-wire service is used to define a virtual wire (E-LINE) connection between two local SAPs or between two SAPs across the SPB network. The SAP that the pseudo-wire service is associated with serves as an attachment point for one end of the point-to-point connection.
  - If the other end of the point-to-point connection is to a local SAP, make sure both SAPs are associated with the same service.
  - If the other end of the point-to-point connection is to a remote SAP, make sure both the local and remote SAP are associated with the same I-SID. This will ensure that there is only one virtual wire connection between the two SPB nodes.
  - Make sure there are no more than two SAP attachment points for the same pseudo-wire service.
Consider the following when configuring an SPB pseudo-wire service and associated SAP:

- Do not configure a pseudo-wire service with the same I-SID on more than two SPB nodes. Configuring the same pseudo-wire service on more than two nodes may cause unpredictable behavior with the connection.
- Configure the SPB pseudo-wire service to use the head-end multicast mode.
- VLAN translation is automatically disabled to ensure packets enter and leave the pseudo-wire connection with the original customer VLAN tag.
- Use the `all` option for the SAP encapsulation (1/1/2:all) to ensure all customer traffic flows through the pseudo-wire connection.
- Flooding and replication are not needed, as there are only two attachment points (SAP to SAP for a local service or SAP to a virtual network port for the same service instance across the SPB backbone network).
- IPv4 over SPB routing, IPv6 over SPB routing, and IGMP snooping are not supported on an SPB pseudo-wire service.
- When an access port that is associated with the Layer 2 profile `def-access-profile` is assigned to an SPB pseudo-wire SAP attachment point, the Layer 2 profile for that port is automatically changed to `pw-def-access-profile`. See the `service access l2profile` command on page page 10-46 for more information.

For more information and configuration examples, refer to the “SPBM Pseudo-Wire (E-LINE Transparent) Service” section of the “Configuring Shortest Path Bridging” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide.

**Examples**

```bash
-> service 100 spb isid 1000 bvlan 4000 pseudo-wire enable description "Pseudo-wire for ISID 1000"
-> service 100 sap port 1/1/1:all

-> service 200 spb isid 2000 bvlan 4000
-> service 200 pseudo-wire enable
-> service 200 sap port 1/1/2:all

-> service 300 spb isid 3000 bvlan 4000
-> service 300 pseudo-wire enable description "Local Pseudo-wire"
-> service 300 sap port 1/1/3:all
-> service 300 sap port 1/1/4:all
```

**Release History**

Release 8.7R2; command was introduced.

**Related Commands**

- `service spb` Configures an SPB service.
- `show service` Displays the service configuration for the bridge.
- `show service ports` Displays the virtual ports (SAPs, SDPs) associated with the service.

**MIB Objects**

- `alaSvcBaseInfoTable`
  - `alaSvcId`
  - `alaSvcType`
  - `alaSvcOption`
alaSvcMacDebugAdminStatus
alaSvcRemoteSystemId
**service vxlan**

Configures a Virtual eXtensible LAN (VXLAN) service. This section describes the base command along with the other optional command keywords that are used to configure VXLAN service parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a `no` form to remove the parameter or return it to its default value.

```
service service_id[-service_id2] vxlan vnid {vxlan_id[-vxlan_id2] | xxx.xxx.xxx[-xxx.xxx.xxx]}
  [description desc_info]
  [multicast-mode [tandem | head-end | hybrid]]
  [stats {enable | disable}]
  [vlan-xlation {enable | disable}]
  [admin-state {enable | disable}]
  [remove-ingress-tag {enable | disable}]
```

```
no service service_id vxlan
```

**Syntax Definitions**

- `service_id[-service_id2]` A unique numerical value to identify a specific VXLAN service. The valid service ID range is 1–32767. Use a hyphen to specify a range of VXLAN services.

- `vxlan_id[-vxlan_id2]` A 24-bit numerical value that identifies a VXLAN segment (a VXLAN network ID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format). Use a hyphen to specify a range of IDs (25001-25005).

**Defaults**

When a VXLAN service is created without specifying any of the optional parameter values, the service is created with the following default values:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>description</code></td>
<td><code>no description added</code></td>
</tr>
<tr>
<td><code>tandem</code></td>
<td><code>hybrid</code></td>
</tr>
<tr>
<td><code>stats</code></td>
<td><code>disable</code></td>
</tr>
<tr>
<td><code>vlan-xlation</code></td>
<td><code>disable</code></td>
</tr>
<tr>
<td><code>admin-state</code></td>
<td><code>disable</code></td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- To remove a VXLAN service, administratively disable the service then use the `no` form of this command and specify the service ID of the disabled service.

- Configuring a VXLAN service on an OmniSwitch 6900-V72/C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported.

- VXLAN services created with this command are considered static services, which are identified by a service ID number between 1 and 32767 (the valid range for this command). If the VXLAN service was dynamically created by another OmniSwitch feature, such as Universal Network Profiles (UNP), a service ID number between 32768 and 65534 is automatically assigned to the dynamic service.

- A VXLAN service provides E-LAN connectivity for customer traffic and is bound to a Service AccessPorts (SAP) on the access side. On the network side, the service is bound to a unicast or multicast Service Distribution Point (SDP).

- Each VXLAN service is basically a Virtual Forwarding Instance (VFI) that is capable of learning customer MAC addresses from the access side (SAPs) and from the network side (mesh SDP) and then switching the traffic based on this information.

Examples

```bash
-> service 10 vxlan vnid 1000 description "VxLAN service for VNID 1000 in hybrid multicast mode" admin-state enable
-> service 20 vxlan vnid 2000 multicast-mode head-end description "VxLAN Service for VNID 2000 in headend mode only" admin-state enable
-> service 30 vxlan vnid 3.173.104 multicast-mode tandem description "VxLAN Service for VNID 3000 in tandem mode only" admin-state enable
-> service 1-100 vxlan vnid 1000-1100 stats enable description "100 VxLAN Services with VNIDs from 1000-1100"
-> no service 20 vxlan
```

Release History

Release 7.3.4; command was introduced.
**Related Commands**

- **service description**
  - Modifies the description information for the service.
- **service multicast-mode**
  - Modifies the multicast replication mode for the service.
- **service stats**
  - Modifies the status of statistics collection for the service.
- **service vxlan-translation**
  - Modifies the status of VLAN translation for the service.
- **service admin-state**
  - Modifies the administrative status for the service.
- **service remove-ingress-tag**
  - Configures whether or not the customer VLAN tag is removed from ingress packets for the specified service.
- **service vxlan udp-port**
  - Configures the UDP destination port for all encapsulated VXLAN frames.
- **service vxlan vrf**
  - Configures the current VRF instance for the VXLAN segment.
- **service sdp vxlan**
  - Manually configures a unicast or multicast VXLAN SDP.
- **service bind-sdp**
  - Binds VXLAN services to VXLAN SDPs.
- **show service**
  - Displays the service configuration for the bridge.

**MIB Objects**

- `alaSvcBaseInfoTable`
  - `alaSvcId`
  - `alaSvcType`
  - `alaSvcVnid`
  - `alaSvcDescription`
  - `alaSvcAdminStatus`
  - `alaSvcAllocationType`
  - `alaSvcStatsAdminStatus`
  - `alaSvcMulticastMode`
  - `alaSvcSapVlanXlation`
**service l2gre**

Configures a Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel service. This type of service is used to define an L2 GRE tunnel endpoint. The service is created and bound to a SAP on an OmniSwitch that will serve as a tunnel aggregation switch.

This section describes the base command along with the other optional command keywords that are used to configure L2 GRE tunnel service parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a `no` form to remove the parameter or return it to its default value.

```plaintext
service service_id l2gre vpnid {vpn_id}
    [description desc_info]
    [stats {enable | disable}]
    [vlan-xlation {enable | disable}]
    [admin-state {enable | disable}]
    [remove-ingress-tag {enable | disable}]

no service service_id l2gre
```

### Syntax Definitions

- **service_id**: A unique numerical value to identify a specific L2 GRE tunnel service. The valid service ID range is 1–32767. Use a hyphen to specify a range of services.

- **vpn_id**: A GRE tunnel Virtual Private Network (VPN) ID. This value should match the VPN ID value used to create the GRE tunnel endpoint on the Guest Tunneling access switch.

### Defaults

When an L2 GRE tunnel service is created without specifying any of the optional parameter values, the service is created with the following default values:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>description desc_info</td>
<td>no description added</td>
</tr>
<tr>
<td>stats {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>vlan-xlation {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>admin-state {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>remove-ingress-tag {enable</td>
<td>disable}</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- To remove an L2 GRE tunnel service, administratively disable the service then use the no form of this command and specify the service ID of the disabled service.

- L2 GRE tunnel services created with this command are considered static services, which are identified by a service ID number between 1 and 32767 (the valid range for this command). If the L2 GRE service was dynamically created by another OmniSwitch feature, such as Universal Network Profiles (UNP), a service ID number between 32768 and 65534 is automatically assigned to the dynamic service.

- An L2 GRE tunnel service provides connectivity for customer traffic and is bound to a SAP on the access side. On the network side, the service is bound to a unicast Service Distribution Point (SDP).

- Each L2 GRE tunnel service is basically a Virtual Forwarding Instance (VFI) that is capable of encapsulating customer MAC addresses from the access side (SAPs) and from the network side (mesh SDP) and then tunneling the traffic through the network.

- L2 GRE tunneling services do not support multicast modes. All Broadcast, Unknown Unicast, and Multicast (BUM) traffic is replicated; a copy is sent to each far-end node over unicast SDPs (similar to the head-end multicast mode).

- On switches that will operate as a tunnel aggregation switch, L2 GRE services and associated service objects are configured through the service l2gre, service sap, service l2gre auto-discover, service sdp l2gre, and service bind-sdp commands.

- On switches that will operate as a tunnel access switch, the L2 GRE service objects are dynamically created based on the specified configuration for a UNP L2 GRE service profile when qualifying device traffic is assigned to that profile. Refer to Chapter 40, “Access Guardian Commands,” in this guide for information about how to configure a UNP L2 GRE service profile.

Examples

- `-> service 10 l2gre vpnid 1000 description "L2GRE service for VPNID 1000" admin-state disable`
- `-> service 20 l2gre vpnid 2000 description "L2GRE service for VPNID 2000" vlan-translation enable admin-state enable`
- `-> service 30 l2gre vpnid 3000 description "L2GRE service for VPNID 3000" remove-ingress-tag enable admin-state enable`
- `-> service 40 l2gre vpnid 4000 description "L2GRE service with VPNID 4000" stats enable admin-state enable`
- `-> service 40 l2gre vpnid 4000 admin-state disable`
- `-> no service 40`
**Release History**

Release 8.4.1.R02; command was introduced.

**Related Commands**

- **service description**
  Modifies the description information for the service.

- **service stats**
  Modifies the status of statistics collection for the service.

- **service vlan-xlation**
  Modifies the status of VLAN translation for the service.

- **service admin-state**
  Modifies the administrative status for the service.

- **service remove-ingress-tag**
  Configures whether or not the customer VLAN tag is removed from ingress packets for the specified service.

- **service l2gre auto-discover**
  Configures the status of L2 GRE automatic SDP discovery on a tunnel aggregation switch. When enabled, the switch discovers the SDPs of remote tunnel end points for a configured L2 GRE service.

- **service sdp l2gre**
  Manually configures an L2 GRE SDP.

- **service bind-sdp**
  Binds L2 GRE services to L2 GRE SDPs.

- **show service**
  Displays the service configuration for the bridge.

**MIB Objects**

- **alaSvcBaseInfoTable**
  - **alaSvcId**
  - **alaSvcType**
  - **alaSvcVpnId**
  - **alaSvcDescription**
  - **alaSvcAdminStatus**
  - **alaSvcAllocationType**
  - **alaSvcStatsAdminStatus**
  - **alaSvcSapVlanXlation**
service description

Configures a description for the specified service.

```
service service_id description desc_info

no service service_id description
```

**Syntax Definitions**

| service_id | An existing service ID number. |
| desc_info  | An ASCII text string up to 160 characters in length. |

**Defaults**

By default, a description is not added when the service is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the description from the specified service ID.
- This command adds or modifies a description for an existing service. However, the `description` parameter is also used to specify a description at the time the service is created.
- Configuring a description for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

**Examples**

Adding or modifying a description for an existing service:

- `service 100 description "SPB service for ISID 1234"`
- `service 200 description "VXLAN service for VNID 24000"`
- `service 300 description "L2GRE service for VPNID 30"`
- `no service 200 description`

Configuring a new service with a description:

- `service 100 isid 1234 bvlan 3000 description "SPB service for ISID 1234"`
- `service 200 vxlan vnid 24000 description "VXLAN service for VNID 24000"`
- `service 300 l2gre vpnid 30 description "L2GRE service for VPNID 30"`
Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

- service spb: Configures an SPB service.
- service vxlan: Configures a VXLAN service.
- service l2gre: Configures an L2 GRE tunnel service.
- service multicast-mode: Configures the multicast replication mode for the specified service.
- service stats: Configures the statistics collection status for the specified service.
- service vlan-xlation: Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
- service admin-state: Configures the administrative status of the specified service.
- show service: Displays the service configuration for the bridge.

MIB Objects

alaSvcBaseInfoTable
  alaSvcId
  alaSvcDescription
service multicast-mode

Configures the multicast replication mode for the specified service.

```
service service_id multicast-mode {head-end | tandem | hybrid}
```

### Syntax Definitions

- **service_id**: An existing service ID number.
- **tandem**: Specifies the tandem replication mode for the service.
- **head-end**: Specifies the head-end replication mode for the service.
- **hybrid**: Specifies the hybrid replication mode for the service. This mode uses both the head-end and tandem methods.

### Defaults

By default, an SPB service is configured to use the head-end mode and a VXLAN service is configured to use the hybrid mode.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When an SPB service is configured to use the head-end mode, a non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address.
- When an SPB service is configured to use the tandem mode, a non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address.
- When configuring IP Multicast Switching (IPMS) for an SPB service, make sure the service was configured to use the head-end multicast mode; IPMS is not supported on SPB services that are configured to use the tandem mode.
- Make sure that the same multicast mode is used across all nodes for a given SPB BVLAN. Tandem nodes and head-end nodes cannot communicate with each other.
- Configuring the multicast mode for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
- Configuring a VXLAN service on an OmniSwitch 6900-V72/C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.
The following multicast mode functionality is supported for VXLAN services:

- **Tandem**: In this mode, PIM multicast routing is required to discover the neighbor nodes and assign membership to VTEP nodes that desire to be in the same multicast group. This requires the manual configuration of a multicast SDP object (an SDP configured with a multicast group address) to tunnel traffic to the other VTEP nodes that belong to the same multicast group.

- **Head-end**: In this mode, unicast SDP objects (SDPs configured with a far-end IP address) are also manually configured to tunnel traffic to the far-end nodes. In this case, however, PIM multicast routing is not required. Any broadcast, unknown unicast, and multicast (BUM) traffic is replicated and one copy is sent to each VTEP node as specified by the unicast SDP object.

- **Hybrid**: In this mode, traffic is tunneled from this service instance to both a group of VTEPs that belong to the same multicast group address and to the VTEP nodes that are not associated with the same multicast group address.

L2 GRE tunneling services do not support multicast modes. All Broadcast, Unknown Unicast, and Multicast (BUM) traffic is replicated; a copy is sent to each far-end node over unicast SDPs (similar to the head-end multicast mode).

This command configures the multicast mode for an existing service. However, the `multicast-mode {head-end | tandem | hybrid}` parameter is also used to specify the status at the time the service is created.

**Examples**

Configuring the multicast mode for an existing service:

```
-> service 100 multicast-mode hybrid
-> service 150 multicast-mode head-end
```

Configuring the multicast mode for a new service:

```
-> service 100 spb isid 2345 bvlan 3000 multicast-mode tandem
-> service 150 vxlan vnid 24000 multicast-mode head-end
```

**Release History**

Release 7.3.1; command was introduced.

Release 7.3.4; VXLAN service support added.
### Related Commands

- **service spb**: Configures an SPB service.
- **service vxlan**: Configures a VXLAN service.
- **service l2gre**: Configures an L2 GRE tunnel service.
- **service description**: Configures a description for the specified service.
- **service stats**: Configures the statistics collection status for the specified service.
- **service vlan-xlation**: Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
- **service admin-state**: Configures the administrative status of the specified service.
- **show service**: Displays the service configuration for the bridge.

### MIB Objects

- **alaSvcBaseInfoTable**
  - **alaSvcId**
  - **alaSvcMulticastMode**
service stats

Configures ingress and egress statistics collection for packets flowing through the service access point (SAP) or service distribution point (SDP) bindings associated with the specified service.

```
 service service_id stats {enable | disable}
```

**Syntax Definitions**

- **service_id**: An existing service ID number.
- **enable**: Administratively enables statistics gathering for the service.
- **disable**: Administratively disables statistics gathering for the service.

**Defaults**

By default, statistics collection is disabled when the service is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command configures statistics collection for an existing service. However, the **stats {enable | disable}** parameter is also used to specify the status at the time the service is created.
- Configuring statistics collection for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-0V72/C32.

**Examples**

Configuring statistics collection for an existing service:
```
-> service 100 stats enable
-> service 100 stats disable
```

Configuring statistics collection for a new service:
```
-> service 200 isid 2345 bvlan 3000 stats enable
-> service 200 isid 3456 bvlan 2000 stats disable
-> service 300 vxlan vnid 24000 stats enable
-> service 300 vxlan vnid 24000 stats disable
-> service 400 l2gre vpnid 40 stats enable
-> service 400 l2gre vpnid 40 stats disable
```
Release History

- Release 7.3.1; command was introduced.
- Release 7.3.4; VXLAN service support added.
- Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

- **service spb**: Configures an SPB service.
- **service vxlan**: Configures a VXLAN service.
- **service l2gre**: Configures an L2 GRE tunnel service.
- **service description**: Configures a description for the specified service.
- **service multicast-mode**: Configures the multicast replication mode for the specified service.
- **service vlan-xlation**: Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
- **service admin-state**: Configures the administrative status of the specified service.
- **show service**: Displays the service configuration for the bridge.

MIB Objects

- `alaSvcBaseInfoTable`
  - `alaSvcId`
  - `alaSvcStatsAdminStatus`
service vlan-xlation

Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.

`service service_id vlan-xlation {enable | disable}`

**Syntax Definitions**

- `service_id` An existing service ID number.
- `enable` Enables VLAN translation for the service.
- `disable` Disables VLAN translation for the service.

**Defaults**

By default, VLAN translation is disabled when the service is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enabling VLAN translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled. The exception to this is on the OmniSwitch 9900, where enabling VLAN translation is required only at the service level.

- Mixing switches with VLAN translation enabled on some and disabled on other switches in the same network is not recommended. When VLAN translation is enabled on a service, all the frames forwarded by the service are treated as untagged within the service domain; the tag is inserted only during egress. As a result, VLAN translation should be enabled for the service across all of the participating switches to prevent frames from egressing the service domain as untagged frames.

- This command configures the VLAN translation status for an existing service. However, the `vlan-xlation {enable | disable}` parameter is also used to specify the status at the time a service is created.

- Configuring VLAN translation for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
**Examples**

Configuring the status for an existing service:

-> service 100 vlan-translation enable
-> service 100 vlan-translation disable

Configuring the status for a new service:

-> service 200 isid 2345 bvlan 3000 vlan-translation enable
-> service 200 isid 3456 bvlan 2000 vlan-translation disable
-> service 300 vxlan vnid 24000 vlan-translation enable
-> service 300 vxlan vnid 24000 vlan-translation disable
-> service 400 12gre vpnid 40 vlan-translation enable
-> service 400 12gre vpnid 40 vlan-translation disable

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

**Related Commands**

- **service spb**
  Configures an SPB service.

- **service vxlan**
  Configures a VXLAN service.

- **service l2gre**
  Configures an L2 GRE tunnel service.

- **service description**
  Configures a description for the specified service.

- **service multicast-mode**
  Configures the multicast replication mode for the specified service.

- **service stats**
  Configures the statistics collection status for the specified service.

- **service admin-state**
  Configures the administrative status of the specified service.

- **show service**
  Displays the service configuration for the bridge.

**MIB Objects**

- **alaSvcBaseInfoTable**
  - **alaSvcId**
  - **alaSvcSapVlanXlation**
service admin-state

Configures the administrative status of the specified service.

**service service_id admin-state {enable | disable}**

### Syntax Definitions

- **service_id**: An existing service ID number.
- **enable**: Administratively enables the service.
- **disable**: Administratively disables the service.

### Defaults

By default, the administrative status is disabled when the service is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Disable the administrative status of the service and any associated service access points (SAPs) and service distribution points (SDPs) before attempting to remove a service.
- Disabling the administrative status does not remove the service configuration from the bridge.
- This command configures the administrative status for an existing service. However, the `admin-state {enable | disable}` parameter is also used to specify the status at the time the service is created.
- Configuring the administrative status for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

### Examples

Configuring the status for an existing service:

```
-> service 100 admin-state enable
-> service 100 admin-state disable
```

Configuring the status for a new service:

```
-> service 200 isid 2345 bvlan 3000 admin-state enable
-> service 200 isid 3456 bvlan 2000 admin-state disable
-> service 300 vxlan v nid 24000 admin-state enable
-> service 300 vxlan v nid 24000 admin-state disable
-> service 400 l2gre v nid 40 admin-state enable
-> service 400 l2gre v nid 40 admin-state disable
```
**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

**Related Commands**

- `service spb` Configures an SPB service.
- `service vxlan` Configures a VXLAN service.
- `service l2gre` Configures an L2 GRE tunnel service.
- `service description` Configures a description for the specified service.
- `service multicast-mode` Configures the multicast replication mode for the specified service.
- `service stats` Configures the statistics collection status for the specified service.
- `service vlan-xlation` Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified service.
- `show service` Displays the service configuration for the bridge.

**MIB Objects**

- `alaSvcBaseInfoTable`  
  - `alaSvcId`  
  - `alaSvcAdminStatus`
service remove-ingress-tag

Configures whether or not the customer VLAN tag is removed from ingress packets for the specified service.

`service service_id remove-ingress-tag {enable | disable}`

### Syntax Definitions

- **service_id**: An existing service ID number.
- **enable**: Customer VLAN tag is removed from ingress packets.
- **disable**: Customer VLAN tag is not removed from ingress packets.

### Defaults

By default, this functionality is disabled when the service is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Removing the customer VLAN tag from ingress packets is particularly useful for services that may forward packets to third-party devices that require untagged packets.

- When this function is enabled, the customer VLAN tag is removed before the packet is encapsulated with a header. The packet is then untagged when the header is removed. For example:
  - The remove ingress tag function is enabled for service 10.
  - Service 10 is associated with SAP 1/2:20 (port 1/2, VLAN tag 20) and SAP 9:30 (link aggregate 9, VLAN tag 30).
  - When a customer packet with VLAN tag 20 enters port 1/1/2, the packet is classified for service 10 and the VLAN 20 tag is removed before the header is added to the untagged packet.
  - When a customer packet with VLAN tag 30 enters link aggregate 9, the packet is classified for service 10 and the VLAN 30 tag is removed before the header is added to the untagged packet.

- This command configures the status of the remove ingress tag functionality for an existing service. However, the `remove-ingress-tag {enable | disable}` parameter is also used to specify the status at the time a service is created.

- Configuring the remove ingress tag status for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
**Examples**

Configuring the status for an existing service:
```
-> service 100 remove-ingress-tag enable
-> service 100 remove-ingress-tag disable
```

Configuring the status for a new service:
```
-> service 200 vxlan vnid 24000 remove-ingress-tag enable
-> service 200 vxlan vnid 24000 remove-ingress-tag disable
-> service 300 l2gre vpnid 25000 remove-ingress-tag enable
-> service 300 l2gre vpnid 25000 remove-ingress-tag disable
```

**Release History**

Release 7.3.4; command was introduced.
Release 8.4.1.R02; L2 GRE tunnel service support added.

**Related Commands**

- `service vxlan` Configures a VXLAN service.
- `service l2gre` Configures an L2 GRE service.
- `show service` Displays the service configuration for the bridge.

**MIB Objects**

- `alaSvcBaseInfoTable`  
  - `alaSvcId`  
  - `alaSvcRemoveIngressTag`
**service vxlan udp-port**

Configures the UDP destination port for all encapsulated VXLAN frames on the gateway switch. Use this command to support previous implementations of the VXLAN functionality that did not use the well-known UDP port 4789. Note that only gateway devices using the same destination UDP port number can exchange encapsulated VXLAN frames.

```
service vxlan udp-port {udp_port_num | default}
```

**Syntax Definitions**

- `udp_port_num` The UDP destination port number to use for VXLAN traffic.
- `default` Use the well-known UDP destination port number (4789) for VXLAN traffic.

**Defaults**

By default, the well-known UDP port number 4789 is used in the default VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Avoid using the well-known UDP ports that are already reserved by IANA for other applications.
- Changing the UDP port number on the fly might stop the VXLAN traffic until the VXLAN Tunnel End Points (VTEPs) in the network are configured with the same destination UDP port.
- Configuring a VXLAN service on an OmniSwitch 6900-V72/C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported.

**Examples**

- `-> service vxlan udp-port 8472`
- `-> service vxlan udp-port default`

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- `service vxlan vrf` Configures the VRF instance for the VXLAN segment.
- `service vxlan` Configures a VXLAN service.
- `show service info` Displays the destination UDP port value applied to VXLAN traffic.

MIB Objects

- `alaSvcMgrSysTable`
  - `alaSvcMgrVxlanDestUdpPort`
**service vxlan vrf**

Configures the current VRF instance for the VXLAN gateway.

```
service vxlan vrf {vrf_name | default}
```

### Syntax Definitions

- **vrf_name**
  - The name of an existing VRF instance.
- **default**
  - Use the default VRF instance.

### Defaults

By default, the default VRF instance is used.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td>X48C6/T48C6/</td>
<td>X48C4E/V48C8/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9900</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Administratively disable all configured SDPs first before changing the VRF instance for the VXLAN segment.
- If the VRF instance that is associated with a VXLAN segment is removed, the VXLAN segment is automatically assigned to the default VRF instance.
- Avoid configuring the same Loopback0 address in multiple VRF instances. Each VRF instance should have a unique Loopback0 address.
- Configuring a VXLAN service on an OmniSwitch 6900-V72/C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported.

### Examples

```
-> service vxlan vrf IpVxlan
-> service vxlan vrf default
```

### Release History

Release 7.3.4; command was introduced.
**Related Commands**

- **service vxlan**  
  Configures a VXLAN service.

- **show service info**  
  Displays the current VRF instance for the VXLAN network.

**MIB Objects**

- **alaSvcMgrSysTable**
  - **alaSvcMgrVxlanCurrentVrf**
service local-vrrp

Configures whether or not the customer VLAN tag is removed from VRRP packets received on SPB service access ports. When enabled, the VLAN tag is automatically removed from the VRRP packets. This is particularly useful when a switch is going to route VRRP packets using IP over SPB.

service local-vrrp {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the TCAM rule (VLAN tag is stripped from VRRP packets received on access ports).</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the TCAM rule (VLAN tag is not stripped from VRRP packets received on access ports).</td>
</tr>
</tbody>
</table>

Defaults

By default, the customer VLAN tag is removed from VRRP packets received on SPB service access ports.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
<tr>
<td>X48C8</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is a global configuration command; the status applies to all access ports on the switch.

- This functionality is enabled to facilitate the processing of VRRP packets received on service access ports on a switch that participates in an IP over SPB routing configuration. When this function is disabled, the customer VLAN tag is not removed from VRRP packets are trapped to the switch for local VRRP processing and are not routed through the IP over SPB configuration.

- When this functionality is enabled (the default), one of the following actions is required based on the switch configuration:
  - If the switch is participating in an IP over SPB routing configuration, enable VLAN translation on all access ports and associated SPB services. This ensures that the VLAN tag is added back into the VRRP packets egressing the access ports.
  - If the switch serves as a transit switch that receives VRRP traffic from another OmniSwitch or a third-party device, use the service local-vrrp command with the disable option to prevent the switch from removing the customer VLAN tag. This helps to avoid having to enable VLAN translation on every single access port and SPB service on the switch.

- When VLAN translation is enabled, a Service Access Point (SAP) with the encapsulation value set to ":all" (all tagged and untagged packets not already assigned) will not work. The ":all" encapsulation value is treated as a ":0" encapsulation value (untagged packets only; tagged packets are dropped) for VLAN translation.
**Examples**

- `-> service local-vrrp disable`
- `-> service local-vrrp enable`

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

- **service access**: Configures a switch port or link aggregate as an access port.
- **service access vlan-xlation**: Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified access port.
- **service vlan-xlation**: Configures the status of egress VLAN translation for the specified service.
- **show service info**: Displays the Service Manager configuration for the local switch.

**MIB Objects**

- `alaSvcMgrSysTable`
  - `alaSvcMgrVrrpMacTcamRuleAdminState`
service l2gre reserved-vlan

Configures a reserved VLAN to activate L2 GRE service domain learning on an L2 GRE tunnel access switch.

```
service l2gre reserved-vlan vlan_id[-vlan_id2]
```

```
no service l2gre reserved-vlan vlan_id[-vlan_id2]
```

**Syntax Definitions**

`vlan_id[-vlan_id2]` A VLAN ID number to configure as an L2 GRE reserved VLAN. Use a hyphen to specify a range of VLAN IDs. The valid range is 2–4092. Up to 8 reserved VLANs can be configured.

**Defaults**

By default, there is no L2 GRE reserved VLAN configured for the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is required only on an OmniSwitch 6560 that serves as an L2 GRE tunnel access switch. A reserved VLAN is not required for other supported OmniSwitch platforms.

- If there is no reserved VLAN configured, UNP does not learn users in the L2 GRE service domain. When a reserved VLAN is created, any blocked users are then learned.

- Use the `no` form of this command to remove an L2 GRE reserved VLAN from the switch configuration. Make sure there are no L2 GRE service objects (SAP, SDP, SDP bindings) configured before attempting to remove the reserved VLAN.

- Specify a VLAN ID that does not already exist in the switch configuration. Use the `show vlan` command to display the VLAN configuration and verify the L2 GRE reserved VLAN configuration.

- The reserved VLAN is used only for L2 GRE learning purposes; other VLAN management operations do not apply to this type of VLAN.

**Examples**

```
-> service l2gre reserved-vlan 4000
-> service l2gre reserved-vlan 4005-4008
-> no service l2gre reserved-vlan 4000
-> no service l2gre reserved-vlan 4005-4008
```
-> service l2gre reserved-vlan 4008-4020
ERROR: VLAN range should be less than or equal to 8.

-> service l2gre reserved-vlan 200
ERROR: Vlan 200 exists. Can not create the vlan!

-> show vlan

<table>
<thead>
<tr>
<th>vlan</th>
<th>type</th>
<th>admin</th>
<th>oper</th>
<th>ip</th>
<th>mtu</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>std</td>
<td>Ena</td>
<td>Dis</td>
<td>Ena</td>
<td>1500</td>
<td>VLAN 1</td>
</tr>
<tr>
<td>200</td>
<td>std</td>
<td>Ena</td>
<td>Dis</td>
<td>Dis</td>
<td>1500</td>
<td>VLAN 200</td>
</tr>
<tr>
<td>500</td>
<td>spb</td>
<td>Ena</td>
<td>Dis</td>
<td>Dis</td>
<td>1524</td>
<td>VLAN 500</td>
</tr>
<tr>
<td>4000</td>
<td>l2gre</td>
<td>Ena</td>
<td>Ena</td>
<td>Dis</td>
<td>1500</td>
<td>L2GRE RESERVED</td>
</tr>
<tr>
<td>4005</td>
<td>l2gre</td>
<td>Ena</td>
<td>Ena</td>
<td>Dis</td>
<td>1500</td>
<td>L2GRE RESERVED</td>
</tr>
<tr>
<td>4006</td>
<td>l2gre</td>
<td>Ena</td>
<td>Ena</td>
<td>Dis</td>
<td>1500</td>
<td>L2GRE RESERVED</td>
</tr>
<tr>
<td>4007</td>
<td>l2gre</td>
<td>Ena</td>
<td>Ena</td>
<td>Dis</td>
<td>1500</td>
<td>L2GRE RESERVED</td>
</tr>
<tr>
<td>4008</td>
<td>l2gre</td>
<td>Ena</td>
<td>Ena</td>
<td>Dis</td>
<td>1500</td>
<td>L2GRE RESERVED</td>
</tr>
<tr>
<td>4094</td>
<td>vcm</td>
<td>Ena</td>
<td>Dis</td>
<td>Dis</td>
<td>1500</td>
<td>VCM IPC</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R4; command was introduced.
Release 8.6R1; configuring a range of L2 GRE reserved VLANs allowed.

**Related Commands**

- **show service info**
  Displays the Service Manager configuration for the local switch.

**MIB Objects**

- alaSvcMgrSysTable
- alaSvcMgrReservedL2greVlan
service l3vpn profile

Configures the status of IP over SPB inline routing support. When enabled (the default), inline routing can be configured on the switch. For more information about inline routing, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide.

service l3vpn profile

no service l3vpn profile

Syntax Definitions

N/A

Defaults

By default, support for IP over SPB service-based inline routing is enabled.

Platforms Supported

This command is supported on the followingOmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C6/T48C6/</td>
<td>X48C6/T48C6/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/</td>
<td>X48C4E/V48C8/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
<td>C32E/T24C2/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
<td>X24C2</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- By default, the OmniSwitch 6800N and OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8 operate in what is referred to as a "Basic" mode in which service-based inline routing is supported. While in the Basic mode, the availability of switch resources is reduced to provide the inline routing support.
- To disable inline routing support, use the no form of this command and then reboot the switch.
- When disabled, inline routing cannot be configured on the switch, however, more system resources are available for other non-inline routing functionality (such as an increase in the number of Layer 3 interfaces, ARPs, etc.).

Examples

-> no service l3vpn profile
WARNING: Reboot needed to change the mode to Disabled

-> service l3vpn profile
WARNING: Changing to current running mode Basic

Release History

Release 8.7R2; command was introduced.
Related Commands

show service l3vpn profile  Displays the status of IP over SPB inline routing support.

MIB Objects

alaCapManServicel3vpnConfig
alaCapManServicel3vpn
**service l2profile**

Configures a Layer 2 profile that is applied to an access (customer facing) port. This profile is used to specify how to process Layer 2 control frames ingressing on the access port.

```
service l2profile l2profile_name [stp | 802.1x | 802.3ad | 802.1ab | mvrp | gvrp | amap] [peer | drop | tunnel]
```

```
no service l2profile profile-name
```

**Syntax Definitions**

- **l2profile_name**
  - Alphanumeric string of up to 32 characters. Use quotes around string if the profile name contains multiple words with spaces between them (e.g., “ALE Engineering”).

- **stp**
  - Specifies how to process Spanning Tree BPDU.

- **802.1x**
  - Specifies how to process 802.1x control frames.

- **802.3ad**
  - Specifies how to process 802.3ad control frames.

- **802.1ab**
  - Specifies how to process 802.1AB control frames. To specify how to process tagged and untagged 802.1AB control frames separately, use the `service l2profile inbound 802.1ab` command.

- **mvrp**
  - Specifies how to process Multiple VLAN Registration Protocol packets.

- **gvrp**
  - Specifies how to process GARP VLAN Registration Protocol packets.

- **amap**
  - Specifies how to process Alcatel-Lucent Enterprise Management Adjacency Protocol packets.

- **peer**
  - Allows the access port to participate in the specified protocol. Control packets are not sent to the network side of the node.

- **drop**
  - Discards the specified PDU.

- **tunnel**
  - Tunnels the specified PDU across the provider network.

**Defaults**

If no parameters are specified with this command, the new profile inherits all the following control protocol settings from the default profile (def-access-profile for service access ports or unp-def-access-profile for UNP access ports):

<table>
<thead>
<tr>
<th>parameter</th>
<th>def-access-profile</th>
<th>unp-def-access-profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>stp</td>
<td>tunnel</td>
<td>drop</td>
</tr>
<tr>
<td>802.1x</td>
<td>drop</td>
<td>peer</td>
</tr>
<tr>
<td>802.3ad</td>
<td>peer</td>
<td>peer</td>
</tr>
<tr>
<td>mvrp</td>
<td>tunnel</td>
<td>tunnel</td>
</tr>
<tr>
<td>gvrp</td>
<td>tunnel</td>
<td>tunnel</td>
</tr>
<tr>
<td>amap</td>
<td>drop</td>
<td>drop</td>
</tr>
<tr>
<td>802.1ab</td>
<td>drop</td>
<td>drop</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to delete a Layer 2 profile. Removing the **def-access-profile** or the **unp-def-access-profile** is not allowed.
- Remove any profile associations with access ports before attempting to modify or delete the profile.
- Not all of the control protocols are currently supported with the **peer**, **tunnel**, and **drop** parameters. Use the following table to determine the parameter combinations that are supported:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Reserved MAC</th>
<th>peer</th>
<th>drop</th>
<th>tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP</td>
<td>01-80-C2-00-00-00</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>802.1x</td>
<td>01-80-C2-00-00-03</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>802.3ad</td>
<td>01-80-C2-00-00-02</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>MVRP</td>
<td>01-80-C2-00-00-21</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>GVRP</td>
<td>01-80-C2-00-00-21</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>AMAP</td>
<td>00-20-DA-00-70-04</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>802.1ab</td>
<td>01-80-C2-00-00-0E</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Examples

- `-> service l2profile sap_1_profile stp drop`
- `-> no service l2profile sap_1_profile`
- `-> service l2profile DropL2`
- `-> service l2profile DropL2 stp drop gvrp drop 802.1ab drop`

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.
Related Commands

```
service access
  Configures a switch port or link aggregate as an access port.

service l2profile inbound 802.1ab
  Configures how tagged and untagged 802.1AB control frames are processed.

service access l2profile
  Assigns a Layer 2 profile to the specified service access port.

unp l2-profile
  Assigns a Layer 2 profile to the specified UNP access port.

show service l2profile
  Displays the Layer 2 profile configuration information for the bridge.
```

MIB Objects

```
alaServiceMgrPortProfileTable
  alaServiceMgrPortProfileID
  alaServiceMgrPortProfileStpBpduTreatment
  alaServiceMgrPortProfile8021xTreatment
  alaServiceMgrPortProfile8021ABTreatment
  alaEServiceUNIProfileGvrpTreatment
  alaServiceMgrPortProfileAmapTreatment
  alaServiceMgrPortProfile8023ADTreatment
```
service l2profile inbound 802.1ab

Configures the treatment of Layer 2 tagged and untagged 802.1AB control frames that are received on access (customer facing) ports. Use this command to specify a different action (peer, drop, or tunnel) based on the tagged and untagged state of an 802.1AB control frame.

service l2profile l2profile_name inbound {tagged | untagged | both} 802.1ab {peer | drop | tunnel}

no service l2profile profile-name

Syntax Definitions

l2profile_name
The name of an existing or new Layer 2 profile.
tagged
The specified action is applied only to tagged 802.1AB control frames.
tagged
The specified action is applied only to untagged 802.1AB control frames.
both
The specified action is applied to both tagged and untagged 802.1AB control frames.
peer
Allows the access port to participate in the 802.1AB protocol. Control packets are not sent to the network side of the node.
drop
Discards 802.1AB PDUs.
tunnel
Tunnels 802.1AB PDUs across the provider network.

Defaults

By default, tagged and untagged 802.1AB control frames are dropped.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to delete the specified Layer 2 profile. Remove any profile associations with access ports before attempting to modify or delete the profile.
- When only the tagged keyword is used, the specified action is applied to tagged traffic and the default action (drop) is applied to untagged traffic.
- When only the untagged keyword is used, the specified action is applied to untagged traffic and the default action (drop) is applied to tagged traffic.
- Only the tunnel and drop actions can be configured for tagged control frames.
• Only the peer and drop actions can be configured for untagged control frames.

• The treatment of 802.1AB control frames received on access ports can either be mixed (different for tagged, different for untagged) or the same for both tagged and untagged control frames. To switch between mixed and the same, set the action for tagged and untagged frames back to the default (drop).

• Use the service l2profile command to configure the treatment for other protocol control frames. This command applies only to 801.1AB frames.

Examples

-> service l2profile lldp-tagged inbound tagged 802.1ab tunnel
-> service l2profile lldp-untagged inbound untagged 802.1ab peer
-> service l2profile lldp-diff inbound tagged 802.1ab tunnel inbound untagged 802.1ab peer
-> service l2profile lldp-both inbound both 802.1ab drop
-> no service l2profile lldp-tagged
-> no service l2profile lldp-untagged
-> no service l2profile lldp-diff
-> no service l2profile lldp-both

Release History

Release 8.6R2; command introduced.

Related Commands

service l2profile Configures a Layer 2 profile that is applied to an access port.
show service l2profile Displays the Layer 2 profile configuration information for the bridge.

MIB Objects

alaServiceMgrPortProfileTable
alaServiceMgrPortProfileID
alaServiceMgrPortProfileStpBpduTreatment
alaServiceMgrPortProfile8021xTreatment
alaServiceMgrPortProfile8021ABTagTreatment
alaServiceMgrPortProfile8021ABUnTagTreatment
alaServiceMgrPortProfile8021ABMode
alaServiceMgrPortProfile8023ADTreatment
alaEServiceUNIProfileGvrpTreatment
alaServiceMgrPortProfileAmapTreatment
alaServiceMgrPortProfileMvrpTreatment
**service access**

Configures a switch port or link aggregate as an access port on which device traffic enters or leaves a service domain.

```
service access {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [description port_description]
```

```
no service access {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `port_description` An alphanumeric string (1–128 characters).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port_description</code></td>
<td>No description</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to revert the port mode back to a regular switch port or link aggregate. Make sure the access port is not associated with any Service Access Points (SAPs) before attempting to change the port mode.

- Use the `no` form of the `description` parameter to remove only the description information from the access port. This option does not remove the access port designation, just the description text that was assigned to the port.

- Before configuring a port or link aggregate as an access port, make sure there is no IP interface configured for the default VLAN of the port. If there is, configuring the port as an access port is not allowed. For example, if VLAN 10 has an IP interface and is the default VLAN for port 1/1/1, then configuring port 1/1/1 as an access port is not supported.
• Access ports are required to configure a SAP. A SAP is the point at which customer traffic enters and exits the service. SAPs are not configurable on other port types.

Examples
-> service access port 1/1/3-10
-> service access linkagg 10-12
-> service access port 1/1/6 description "Voice Access Port"
-> service access port 2/1/6 description "L3 VPN Loopback Port"
-> service access linkagg 100 description "Server Access Port"
-> service access port 2/1/6 no description
-> no service access port 1/1/3
-> no service access linkagg 10

-> vlan 100
-> ip interface v100 address 10.10.10.1 vlan 100
-> vlan 100 members port 1/1/1 untagged
-> service access port 1/1/1
ERROR: A vlan with IP interface attached to this port is not supported!

Release History
Release 7.3.1; command was introduced.
Release 7.3.2; description parameter added.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands
service l2profile
Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames that ingress on the access port.

service access l2profile
Assigns a Layer 2 profile to the specified service access port.

service access vlan-xlation
Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified access port.

show service access
Displays the access (customer-facing) port configuration for the bridge.

MIB Objects
alaServiceMgrPortTable
alaServiceMgrPortID
alaServiceMgrPortMode
alaServiceMgrPortDescription
service access l2profile

Assigns an existing Layer 2 profile to the specified service access port. This profile determines how Layer 2 protocol frames received on the access port are processed.

service access {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} l2profile {default | profile-name}

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **default**: Assigns the default profile to the specified port.
- **profile-name**: The name of an existing Layer 2 profile.

Defaults

By default, the default Layer 2 profile (**def-access-profile**) is assigned when a port is configured as a service access port.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **default** parameter with this command to revert the associated profile back to the default profile settings.
- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to network ports.
- Specify a profile name that already exists in the switch configuration.
- If a user-configured Layer 2 profile is not associated with a service access port, then the **def-access-profile** is used to process control packets that ingress on the service access port.
- If a user-configured Layer 2 profile is not associated with a UNP access port, then the **unp-def-access-profile** is used to process control packets that ingress on the UNP access port. To assign a Layer 2 profile to a UNP access port, use the **unp l2-profile** command.
When a service access port is configured with the **def-access-profile** and then assigned to an SPB pseudo-wire SAP, the Layer 2 profile for that port automatically changes to **pw-def-access-profile** and the following control protocol settings are used to process ingress control packets:

<table>
<thead>
<tr>
<th>parameter</th>
<th>def-access-profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>stp</td>
<td>tunnel</td>
</tr>
<tr>
<td>802.1x</td>
<td>tunnel</td>
</tr>
<tr>
<td>802.3ad</td>
<td>peer</td>
</tr>
<tr>
<td>mvrp</td>
<td>tunnel</td>
</tr>
<tr>
<td>gvrp</td>
<td>tunnel</td>
</tr>
<tr>
<td>amap</td>
<td>tunnel</td>
</tr>
<tr>
<td>802.1ab</td>
<td>tunnel</td>
</tr>
</tbody>
</table>

- If a user-configured Layer 2 profile is associated with a service access port that is then assigned to an SPB pseudo-wire SAP, the Layer 2 profile for that port is *not* changed. The user-configured profile is applied to control packets received on the port, not the **pw-def-access-profile**.
- When the **default** parameter is used, the Layer 2 profile assignment for the service access port reverts back to **def-access-profile**, regardless of whether the port was assigned to a user-configured profile or to **pw-def-access-profile**.
- Removing the **pw-def-access-profile** is not allowed.
- See the **service pseudo-wire** command on page page 10-7 for more information.

**Examples**

- `-> service access port 1/1/3 l2profile sap_1_profile`
- `-> service access linkagg 10 l2profile sap_1_profile`
- `-> service access port 1/1/3 l2profile default`
- `-> service access linkagg 10 l2profile default`

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.
Release 8.7R2; **pw-def-access-profile** added for SPB pseudo-wire access ports.
Related Commands

**service access**  
Configures a switch port or link aggregate as an access port.

**service l2profile**  
Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.

**show service l2profile**  
Displays the Layer 2 profile configuration information for the bridge.

**show service access**  
Displays the access (customer-facing) port configuration for the switch.

MIB Objects

alaServiceMgrPortTable
  - alaServiceMgrPortID
  - alaServiceMgrPortMode
  - alaServiceMgrPortPortProfileID
service access vlan-xlation

Configures the status of egress VLAN translation for all the service access points (SAPs) associated with the specified access port.

`service access {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} vlan-xlation {enable | disable}`

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **enable**: Enables VLAN translation for the specified port.
- **disable**: Disables VLAN translation for the specified port.

**Defaults**

By default, VLAN translation is disabled when a port or link aggregate is configured as an access port.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify only ports or link aggregates that are configured as service access ports. This command does not apply to interfaces configured as network ports.
- Enabling VLAN translation on an access port implicitly enables translation for all SAPs associated with that port. However, translation must also be enabled for the services associated with these SAPs. This ensures that all SAPs associated with a service will apply VLAN translation.
- On an OmniSwitch 9900, VLAN translation is configured only at the service level; configuring access port level VLAN translation is not required.
- Mixing switches with VLAN translation enabled on some and disabled on other switches in the same network is not recommended. When VLAN translation is enabled on a service, all the frames forwarded by the service are treated as untagged within the service domain; the tag is inserted only during egress. As a result, VLAN translation should be enabled for the service across all the participating switches to prevent frames from egressing the service domain as untagged frames.
**Examples**

-> service access port 1/3 vlan-xlation enable
-> service access linkagg 10 vlan-xlation enable
-> service access port 1/3-10 vlan-xlation disable
-> service access linkagg 10-15 vlan-xlation disable

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

**Related Commands**

- `service access`  
  Configures a switch port or link aggregate as an access port.
- `service vlan-xlation`  
  Configures the status of egress VLAN translation for the specified service.
- `show service access`  
  Displays the access (customer-facing) port configuration for the switch.

**MIB Objects**

`alaServiceMgrPortTable`
- `alaServiceMgrPortID`
- `alaServiceMgrPortMode`
- `alaServiceMgrPortVlanXlation`
service sap

Configures a Service Access Point (SAP) by associating a SAP ID with a Shortest Path Bridging (SPB) service, a Virtual eXtensible LAN (VXLAN) service, or a Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel service. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of network traffic to map to the associated service.

This section describes the base command along with the other optional command keywords that are used to configure SAP parameter values. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a no form to remove the parameter or return it to its default value.

```
service service_id sap {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [sap_id]
[description desc_info]
[tcp-mss {overlay-profile {spb | ethernet} | num}]
[trusted | un-trusted [priority]]
[stats {enable | disable}]
[admin-state {enable | disable}]
```

```
no service service_id sap {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [sap_id]
```

Syntax Definitions

- **service_id**: An existing SPB, VXLAN, or L2 GRE service ID number.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **sap_id**: The SAP ID (chassis/slot/port:encapsulation). Refer to the table in the “Usage Guidelines” section of this command page for a list of encapsulation values to select for the SAP ID.
- **spb | ethernet | num**: The TCP Maximum Segment Size (tcp-mss) size. **spb** (1380), **ethernet** (1402), **num** (500-1410)

## Defaults

When a SAP is created without specifying any optional parameter values, the SAP is created with the following defaults:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>:0</td>
<td>:all</td>
</tr>
<tr>
<td>description desc_info</td>
<td>No description added</td>
</tr>
<tr>
<td>trusted</td>
<td>un-trusted [priority]</td>
</tr>
<tr>
<td>stats enable</td>
<td>disable</td>
</tr>
<tr>
<td>admin-state enable</td>
<td>disable</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to remove a SAP from the specified service.

- To define the SAP ID that will be associated with the SPB, VXLAN, or L2 GRE service, enter the access port or link aggregate number followed by one of the following encapsulation values (for example, service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID):

<table>
<thead>
<tr>
<th>SAP ID Encapsulation</th>
<th>Customer Traffic Forwarded by the SAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>:0</td>
<td>Specifies a null encapsulation value for the SAP. All untagged traffic is mapped to the SAP; tagged traffic is dropped.</td>
</tr>
<tr>
<td>:all</td>
<td>Specifies a wildcard SAP. All tagged and untagged traffic that is not classified into another SAP is mapped to the wildcard SAP.</td>
</tr>
<tr>
<td>:qtag[-qtag2]</td>
<td>Specifies a VLAN ID tag for ingress traffic on the access port. Only traffic with this 802.1Q tag is mapped to the SAP. Use a hyphen to specify a range of VLAN IDs (21-30).</td>
</tr>
<tr>
<td>:outer_qtag.inner_qtag</td>
<td>Specifies an outer VLAN ID tag and an inner VLAN tag for ingress traffic on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.</td>
</tr>
</tbody>
</table>

- The **:all** (wild card) parameter is also configurable as the inner tag value for double-tagged packets (for example, “10:all” specifies double-tagged packets with an outer tag equal to VLAN 10 and an inner tag with any VLAN ID value).

- When VLAN translation is enabled, a Service Access Point (SAP) with the encapsulation value set to ":all" (all tagged and untagged packets not already assigned) will not work. The ":all" encapsulation value is treated as a ":0" encapsulation value (untagged packets only; tagged packets are dropped) for VLAN translation.

- Specify only ports or link aggregates that are configured as service access ports (see **service access**). This command does not apply to network ports.

- Configuring SAPs with different encapsulation types for the same access port is allowed.

- When specifying a range of VLAN IDs with this command on an OmniSwitch 6900-X72/Q32, consider the following guidelines:
  - Each service access port supports a maximum of 8 SAPs that are created with a range of VLANs.
  - A total of 255 service access ports can support a range of VLANs at any given time.
  - The range of VLANs specified for the SAPs of a service access port cannot overlap each other.
  - For double-tagged SAPs, separate range commands can be specified for both outer and inner VLAN tags.
– The outer VLAN range space is shared with the same space as QTAG SAP. The combined limit is 8 unique ranges per service access port. This is in addition to the 8 unique inner VLAN range per service access port.

- When configuring a SAP for a VXLAN service, consider the following:
  – Configuring a VXLAN SAP is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
  – Configuring a VXLAN service on an OmniSwitch 6900-V72/C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.

- When configuring a SAP for an L2 GRE tunnel, consider the following:
  – A SAP is manually configured on a tunnel aggregation switch through the **service sap** command.
  – A SAP is dynamically created on a tunnel access switch based on the L2 GRE tunnel service parameters mapped to the UNP profile when qualifying device traffic is assigned to the profile. Refer to Chapter 40, “Access Guardian Commands,” for information about how to configure a UNP L2 GRE service profile.

- The TCP Maximum Segment Size (TCP-MSS) carried in the TCP SYN/SYN-ACK frames can be configured to set an MTU value supported by a VXLAN tunnel.

**Examples**

```
-> service 100 sap port 1/1/1:0
-> service 100 sap port 1/1/1:50 description “Server1 to VXLAN10 SAP”
-> service 100 sap port 1/2/10:100.200 admin-state enable
-> service 100 sap port 1/2/10:500.all untrusted stats enable
-> service 100 sap linkagg 5:10
-> service 200 sap linkagg 2:20:30
-> service 200 sap linkagg 9:all untrusted 3 stats enable admin-state enable
-> no service 100 sap port 1/1/1:50 description
-> no service 100 sap port 1/2/10:100.200
-> no service 200 sap linkagg 9:all

-> service 10 sap port 1/1/11-20:21-30 description “SAPs on ports 1/1/11 to 1/1/20 with tag 21 to 30”
-> service 20 sap linkagg 1-10:100 un-trusted description “Untrusted SAPs for lag 1-10 with tag 100”
-> service 30 sap port 1/1/2:10-20 description “SAP on port 1/1/2 with only one VP for tag 10-20”
-> service 30 sap linkagg 11:10-20 description “SAP on lag 11 with only one VP for tag 10-20”
-> service 1 sap port 1/1/7:all un-trusted 0 tcp-mss 1300 description “Untrusted SAPs on port 1/1/7 for all traffic and maximum segment size of 1300”
```

**Release History**

Release 7.3.1.; command was introduced.
Release 7.3.4.; support for entering a range of SAP ports, link aggregates, and VLAN ID tags added; VXLAN service support added).
Release 8.4.1.R02; support for L2 GRE tunnel services added.
**Related Commands**

- `service sap description`  
  Configures a description for the specified SAP ID.

- `service sap trusted`  
  Configures the trust mode for the specified SAP ID.

- `service sap stats`  
  Configures statistics collection for the specified SAP ID.

- `service sap admin-state`  
  Configures the administrative status for the specified SAP ID.

- `service spb`  
  Configures an SPB service.

- `service vxlan`  
  Configures a VXLAN service.

- `service l2gre`  
  Configures an L2 GRE tunnel service.

- `service access`  
  Configures a service access port.

- `show service ports`  
  Displays SAP configuration information for the specified service.

**MIB Objects**

- `alaSapBaseInfoTable`  
  `alaSapSvcId`
  `alaSapPortId`
  `alaSapEncapValue`
  `alaSapType`
  `alaSapDescription`
  `alaSapTrusted`
  `alaSapPriority`
  `alaSapStatsAdminStatus`
  `alaSapAdminStatus`
**service sap description**

Configures a description for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

```
service service_id sap {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [:0 | :all | :qtag[-qtag2] | :outer_qtag.inner_qtag} description desc_info
```

```
no service service_id sap {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [:0 | :all | :qtag[-qtag2] | :outer_qtag.inner_qtag} description
```

**Syntax Definitions**

- **service_id**
  - An existing SPB, VXLAN, or L2 GRE service ID number.

- **chassis**
  - The chassis identifier when running in virtual chassis mode.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **:0**
  - Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.

- **:all**
  - Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.

- **:qtag[-qtag2]**
  - Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30).

- **:outer_qtag.inner_qtag**
  - Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.

- **desc_info**
  - An ASCII text string up to 160 characters in length.

**Defaults**

By default, a description is not added when the SAP is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

OmniSwitch AOS Release 8 CLI Reference Guide    April 2023    page 10-55
Usage Guidelines

- Use the `no` form of this command to remove the description from the specified SAP.
- Specify the service ID number associated with the specified SAP ID (access port/encapsulation).
- Configuring a description for a VXLAN SAP is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

Examples

```
-> service 10 sap port 1/2:10 description "CE1 to SPB10 SAP"
-> service 13 sap linkagg 20:100.200 description "CE2 to SPB13 SAP"
-> service 15 sap port 1/11-20:21-30 description "SAPs on ports 1/11 to 1/20 with tag 21 to 30"
-> service 30 sap port 1/2:10-20 description "SAP on port 1/2 with only one VP for tag 10-20"
-> service 10 sap port 1/2:10 no description
-> service 13 sap linkagg 20:100.200 no description
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkaggs, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.

Related Commands

```
service sap configures a SAP by associating a SAP ID with a SPB service.
service sap trusted configures the trust mode for the specified SAP ID.
service sap stats configures statistics collection for the specified SAP ID.
service sap admin-state configures the administrative status for the specified SAP ID.
show service ports displays SAP configuration information for the specified service.
```

MIB Objects

```
alaSapBaseInfoTable
   alaSapPortId
   alaSapEncapValue
   alaSapDescription
   alaSapSvcId
```
**service sap trusted**

Configures the trust mode for the specified Service Access Port (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

A trusted SAP can accept 802.1p values in incoming packets; an untrusted SAP will set any 802.1p values to zero in incoming packets, unless an 802.1p value is configured with this command.

```
service service_id sap {port chassis/slot/port | linkagg agg_num} [:0 | :all | :qtag |
:outer_qtag:inner_qtag] {trusted | un-trusted [priority]}
```

### Syntax Definitions

- **service_id**
  - An existing SPB, VXLAN, or L2 GRE service ID number.

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **:0**
  - Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.

- **:all**
  - Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.

- **:qtag[-qtag2]**
  - Specifies a VLAN ID tag for traffic received on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30).

- **:outer_qtag:inner_qtag**
  - Specifies an outer VLAN ID tag and an inner VLAN tag for traffic received on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.

- **trusted**
  - Allows the SAP to use the priority value obtained from tagged packets received on the SAP port. Untagged packets use the default port priority value.

- **un-trusted**
  - Sets the priority value to zero for tagged and untagged packets received on the SAP. This is the priority assigned to tagged and untagged packets received on an untrusted SAP.

- **priority**
  - The priority value to set for tagged and untagged packets received on an untrusted SAP. Values range from 0 (lowest priority) to 7 (highest priority).

### Defaults

By default, the SAP is trusted with the priority set to best effort (zero). These default values are set when a port is configured as an access port and then associated with the SAP.
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `un-trusted` and the `priority` parameter options to assign an 802.1p priority value to ingress packets processed by the SAP. When the `un-trusted` parameter is used without specifying a priority value, a value of zero is automatically assigned to the ingress packets.

- Specify the service ID number associated with the specified SAP ID (access port/encapsulation).

- Administratively disabling the SAP is not required to change the trust mode for the SAP.

- When the trust mode is changed from untrusted to trusted, the priority value is automatically set to the default best effort priority value (zero).

- Note that untagged Layer 2 control packets (for example, BPDUs, GVRP, and AMAP) are always tunneled (if enabled) through the provider backbone bridge (PBB) network with the default EXP bits set to 7, so that they can arrive at the destination bridge at the highest COS queue of 7. As a result, trusted and untrusted SAPs configured on the access ports will not affect the Layer 2 control packets ingressing on the access ports.

- Configuring the trust mode on an access port is not allowed. These settings are configured for the SAP to which the access port is associated.

- Configuring the trust mode for a VXLAN SAP is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

Examples

```
-> service 10 sap port 1/1/2:10 trusted
-> service 13 sap linkagg 20 trusted
-> service 10 sap port 1/1/2:10 un-trusted
-> service 13 sap linkagg 20 un-trusted 5
-> service 20 sap linkagg 1-10:100 un-trusted
-> service 30 sap linkagg 11:10-20 trusted
```

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkagg, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.
Related Commands

- `service sap` Configures a SAP by associating a SAP ID with a SPB service.
- `service sap description` Configures a description for the specified SAP ID.
- `service sap stats` Configures statistics collection for the specified SAP ID.
- `service sap admin-state` Configures the administrative status for the specified SAP ID.
- `show service ports` Displays SAP configuration information for the specified service.

MIB Objects

- `alaSapBaseInfoTable`
  - `alaSapPortId`
  - `alaSapEncapValue`
  - `alaSapTrusted`
  - `alaSapPriority`
  - `alaSapSvcId`
**service sap stats**

Configures ingress and egress statistics collection for packets flowing through the specified SAP ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

```
service service_id sap {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} {:0 | :all | :qtag[-qtag2] | :outer_qtag.inner_qtag} stats {enable | disable}
```

**Syntax Definitions**

- **service_id**: An existing SPB, VXLAN, or L2 GRE service ID number.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **:0**: Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
- **:all**: Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
- **:qtag[-qtag2]**: Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30).
- **:outer_qtag.inner_qtag**: Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
- **enable**: Enables statistics collection for the SAP.
- **disable**: Disables statistics collection for the SAP.

**Defaults**

By default, statistics collection is disabled for the SAP.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify the service ID number associated with the specified SAP ID (access port/encapsulation).
Configuring statistics collection for a VXLAN SAP is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

**Examples**

-> service 100 sap port 1/1/2:10 stats enable
-> service 101 sap linkagg 20:all stats enable
-> service 100 sap port 1/1/2:10 stats disable
-> service 101 sap linkagg 20:all stats disable
-> service 10 sap port 1/11-20:21-30 stats enable
-> service 30 sap linkagg 11:10-20 stats disable

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkaggs, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.

**Related Commands**

- service sap
  - Configures a SAP by associating a SAP ID with a SPB service.
- service sap description
  - Configures a description for the specified SAP ID.
- service sap trusted
  - Configures the trust mode for the specified SAP ID.
- service sap admin-state
  - Configures the administrative status for the specified SAP ID.
- show service ports
  - Displays SAP configuration information for the specified service.

**MIB Objects**

- alaSapBaseInfoTable
- alaSapPortId
- alaSapEncapValue
- alaSapStatsAdminStatus
- alaSapSvcId
### service sap admin-state

Configures the administrative status for the specified Service Access Point (SAP) ID. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

```
service service_id sap {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} {:0 | :all | :qtag[-qtag2] | :outer_qtag.inner_qtag} admin-state {enable | disable}
```

#### Syntax Definitions

- **service_id**: An existing SPB, VXLAN, or L2 GRE service ID number.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **:0**: Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
- **:all**: Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
- **:qtag[-qtag2]**: Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP. Use a hyphen to specify a range of VLAN IDs (21-30)
- **:outer_qtag.inner_qtag**: Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
- **enable**: Enables the administrative status for the SAP.
- **disable**: Disables the administrative status for the SAP.

#### Defaults

By default, the administrative status of the SAP is enabled.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- Specify the service ID number associated with the specified SAP ID (access port/encapsulation).
• Disabling the SAP administrative status does not remove the SAP configuration from the bridge.
• If an access port goes down, all SAPs associated with that port are operationally taken down as well.
• Configuring the administrative status for a VXLAN SAP is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

Examples
-> service 10 sap port 1/2:10 admin-state enable
-> service 13 sap linkagg 20 admin-state enable
-> service 10 sap port 1/2:10 admin-state disable
-> service 13 sap linkagg 20 admin-state disable
-> service 10 sap port 1/11-20:21-30 admin-state enable
-> service 30 sap linkagg 11:10-20 admin-state disable

Release History
Release 7.3.1; command was introduced.
Release 7.3.4; support for entering a range of SAP ports, linkaggs, and VLAN ID tags added; VXLAN service support added.
Release 8.4.1.R02; support for L2 GRE tunnel services added.

Related Commands

service sap
    Configures a SAP by associating a SAP ID with a SPB service.

service description
    Configures a description for the specified SAP ID.

service sap trusted
    Configures the trust mode for the specified SAP ID.

service sap stats
    Configures statistics collection for the specified SAP ID.

show service ports
    Displays SAP configuration information for the specified service.

MIB Objects

alaSapBaseInfoTable
alaSapPortId
alaSapEncapValue
alaSapAdminStatus
alaSapSvcId
**service sdp vxlan**

Configures a Service Distribution Point (SDP) for Virtual eXtensible LAN (VXLAN) traffic. This type of SDP is used to tunnel unicast or multicast traffic between VXLAN Tunnel End Points (VTEPs). Configuring an SDP is automatically done for Shortest Path Bridging (SPB) services; this command is only for VXLAN services.

```
service sdp sdp_id vxlan {far-end ip_address | multicast-group mc_group_address} [ttl {ttl_num | default}] [description desc_info] [admin-state {enable | disable}]
```

```
no service sdp sdp_id [description]
```

**Syntax Definitions**

- **sdp_id**: The ID number to assign to the SDP object.
- **ip_address**: The IP address of the Loopback0 interface for the far-end VTEP node. The Loopback0 address is required on every VTEP node.
- **mc_group_address**: The multicast IP address of the group to which this service will join. This parameter is not supported on an OmniSwitch 6900-V72/C32.
- **ttl_num**: A Time-to-Live (TTL) value that is inserted into the TTL field of the IP header when the VXLAN encapsulated frames are sent from this node. The valid range is 1–255.
- **default**: Sets the TTL value to the default value of 64.
- **desc_info**: An ASCII text string up to 160 characters in length.
- **enable**: Enables the administrative status of the SDP.
- **disable**: Disables the administrative status of the SDP.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ttl {default</td>
<td>ttl_num}</td>
</tr>
<tr>
<td>description desc_info</td>
<td>No description.</td>
</tr>
<tr>
<td>admin-state {enable</td>
<td>disable}</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 10-64
Usage Guidelines

- Use the **no** form of this command to delete the SDP object, only if the SDP is not bound to any services. If the **description** parameter is specified with the **no** form, then only the description information is removed from the SDP.

- When the **far-end** option is used, this command specifies a single destination unicast IP address that identifies the far-end VTEP node to which the SDP will tunnel traffic. This IP address is the Loopback0 address configured on every VTEP node. The SDP is then bound to a VXLAN service to direct one-way VXLAN encapsulated traffic to that single far-end node. This object is similar to the unicast SDP in SPB.

- When the **multicast-group** option is used, this command specifies the multicast group address to which all broadcast, unknown unicast, and multicast (BUM) traffic is sent to the VTEP nodes that subscribe to the PIM multicast group will receive this type of traffic. In this mode, the **ttl** parameter value is included in the IP header of the VXLAN encapsulation header:

- If the IP address of a VTEP node is learned, thus creating a dynamic unicast SDP through the discovery process, the unicast traffic is sent to the VTEP node that is associated with that learned IP address. This object is similar to multicast SDP in SPB.

- The administrative status of the VXLAN SDP affects all SDP bindings that are bound to this object.

- Configuring a VXLAN service on an OmniSwitch 6900-V72/C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. As a result, creating an SDP with a multicast group address is also not supported (tandem mode services are bound to multicast SDPs).

Examples

```
-> service sdp 10 vxlan multicast-group 224.2.1.1 ttl 20 description "PIM Group 224.2.1.1"
-> service sdp 10 ttl 5
-> service sdp 20 far-end 10.10.10.2 description "Unicast to NodeB"
-> service sdp 20 admin-state disable
-> no service sdp 10 description
-> no service sdp 10
```

Release History

Release 7.3.4; command was introduced.

Related Commands

- **service bind-sdp** Binds VXLAN services to VXLAN SDPs.
- **service vxlan** Configures a VXLAN service.
- **show service sdp** Displays the SDP configuration for the switch.
- **show service bind-sdp** Displays the service-to-SDP binding configuration for the switch.
MIB Objects

alaSdpInfoTable
  alaSdpId
  alaSdpRowStatus
  alaSdpSvcType
  alaSdpFarEndIpAddress
  alaSdpDescription
  alaSdpAdminStatus
  alaSdpAllocationType
  alaSdpDynamicType
  alaSdpAdminTTL
service sdp l2gre

Configures a Service Distribution Point (SDP) for Layer 2 Generic Routing Encapsulation (L2 GRE) traffic. This type of SDP is used to tunnel encapsulated GRE traffic between two L2 GRE tunnel end points. Manual configuration of an L2 GRE SDP is required on a switch serving as a tunnel aggregation switch.

```
service sdp sdp_id l2gre far-end ip_address [ttl {ttl_num | default}] [description desc_info] [admin-state {enable | disable}]
```

```
no service sdp sdp_id [description]
```

**Syntax Definitions**

- `sdp_id`  
  The ID number to assign to the SDP object.

- `ip_address`  
  The IP address of the Loopback0 interface for the far-end Guest Tunnel access switch. The Loopback0 address is required on every Guest Tunnel endpoint.

- `ttl_num`  
  A Time-to-Live (TTL) value that is inserted into the TTL field of the GRE header when the GRE encapsulated frames are sent from this node. The valid range is 1–255.

- `default`  
  Sets the TTL value to the default value of 64.

- `desc_info`  
  An ASCII text string up to 160 characters in length.

- `enable`  
  Enables the administrative status of the SDP.

- `disable`  
  Disables the administrative status of the SDP.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ttl {default</td>
<td>ttl_num}`</td>
</tr>
<tr>
<td><code>description desc_info</code></td>
<td>No description.</td>
</tr>
<tr>
<td>`admin-state {enable</td>
<td>disable}`</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the no form of this command to delete the SDP object, only if the SDP is not bound to any services. If the description parameter is specified with the no form, then only the description information is removed from the SDP.

- The far-end IP address value specifies a single destination unicast IP address that identifies the far-end L2 GRE tunnel access switch to which the SDP will tunnel traffic. This IP address is the Loopback0 interface address configured on every tunnel end point. The SDP is then bound to an L2 GRE service to direct one-way GRE encapsulated traffic to that single far-end tunnel access switch. This object is similar to the unicast SDP in SPB, however, multicast SDPs are not configurable for L2 GRE tunneling.

- The administrative status of the L2 GRE SDP affects all SDP bindings that are bound to this object.

- When L2 GRE automatic SDP discovery is enabled (the default), manual configuration of the SDP and SDP binding is not required on the L2 GRE tunnel aggregation switch (see the service l2gre auto-discover command for more information).

- Configuring L2 GRE tunneling on an OmniSwitch 6900-T20/T40 or OmniSwitch 6900-X20/X40 is recommended when these models are part of a mixed VC and the L2 GRE SDP is configured on one of the other switches in the mixed VC (for example, on an OmniSwitch 6900-X72/Q32 or OmniSwitch 6900-V72/C32). This ensures that all routing and multicast functionality required to support an L2 GRE tunnel service is limited to a switch that supports SDP configuration.

Examples

-> service sdp 20 l2gre far-end 192.168.0.10 admin-state enable description "Guest SDP to access switch 192.168.0.10"
-> service sdp 20 ttl 5
-> service sdp 20 admin-state disable
-> no service sdp 20 description
-> no service sdp 20

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

- service bind-sdp
  Binds VXLAN services to VXLAN SDPs.
- service l2gre
  Configures an L2 GRE tunnel service.
- show service sdp
  Displays the SDP configuration for the switch.
- show service bind-sdp
  Displays the service-to-SDP binding configuration for the switch.

MIB Objects

alaSdpInfoTable
  - alaSdpId
  - alaSdpSvcType
  - alaSdpCreationOrigin
  - alaSdpFarEndIpAddress
  - alaSdpDescription
  - alaSdpAdminStatus
  - alaSdpAdminTTL
alaSdpRowStatus
**service bind-sdp**

Configures the binding of a Virtual eXtensible LAN (VXLAN) service or a Layer 2 Generic Encapsulation Routing (L2 GRE) tunnel service to a Service Distribution Point (SDP).

```
service service_id bind-sdp sdp_id1 [sdp_id2 sdp_id3 ...] [description desc_info]
service service_id[-service_id2] bind-sdp sdp_id [description desc_info]
no service service_id bind-sdp sdp_id [description]
```

**Syntax Definitions**

- `service_id[-service_id2]` An existing VXLAN service ID or an L2 GRE tunnel service ID to bind to the SDP. Use a hyphen to specify a range of services to bind to the SDP.
- `sdp_id` An existing SDP ID number to bind to the service. Use a space to specify additional SDP IDs to bind to the specified service (for example, 10 20 30 40 50).
- `desc_info` An ASCII text string up to 160 characters in length.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>desc_info</td>
</tr>
<tr>
<td>desc_info</td>
<td>No description.</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the SDP binding. If the `description` parameter is specified with the `no` form, then only the description information is removed from the SDP binding.
- There is no control of the SDP administrative status; this type of service object is always enabled.
- Only static SDPs (created with an SDP ID between 1–32767) can be manually bound to a VXLAN service or an L2 GRE tunnel service; otherwise, an error message is returned.
- When configuring an SDP binding for a VXLAN service, consider the following:
  - VXLAN is only supported on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
  - An SDP binding is defined to allow VXLAN traffic to reach other nodes in the same group (multicast SDP) or reach a single node (unicast SDP).
A tandem mode VXLAN service can be bound only to one multicast SDP (not supported on an OmniSwitch 6900-V72/C32).

A head-end mode VXLAN service can be bound only to unicast SDPs.

A hybrid mode service can be bound with one multicast SDP for a group of member VTEPs and with many unicast SDPs for VTEPs that do not participate in a multicast group.

On an OmniSwitch 6900-V72/C32, only head-end mode VXLAN services are supported. As a result, creating an SDP bind for a tandem mode service is not supported on this platform. If the service is configured to use the hybrid multicast mode, then the service can only be bound to a unicast SDP.

- When configuring an SDP binding for an L2 GRE tunnel service, consider the following:
  - An SDP and SDP binding is defined on a tunnel aggregation switch to allow L2 GRE tunnel traffic to reach a single tunnel access switch (unicast SDP).
  - One SDP and SDP binding is configured for each tunnel access switch that will tunnel traffic to the tunnel aggregation switch.
  - When L2 GRE automatic discovery is enabled (the default), manual configuration of the SDP and SDP binding is not required on the L2 GRE tunnel aggregation switch (see the service l2gre autocDiscover command for more information).

Examples

```plaintext
-> service 1 bind-sdp 10 description "Bind to PIM Group 224.2.1.1"
-> service 2 bind-sdp 20 description "Unicast Bind to 1.1.1.20 VTEP"
-> service 4 bind-sdp 30 description "Unicast Bind to 10.2.2.1 Guest Access Switch:
-> service 5 bind-sdp 40 50 60 70 80 90
-> service 1-100 bind-sdp 10 description "Bind Services 1-100 to PIM Group 225.2.1.1"
-> service 200-250 bind-sdp 20 description "Bind Services 200-250 to 1.1.1.20 VTEP"
-> service 300-350 bind-sdp 30 description "Bind Services 300-350 to 10.2.2.1 Guest Access Switch"
-> no service 1 bind-sdp 10 description
-> no service 2 bind-sdp
```

Release History

Release 7.3.4; command was introduced.
Release 8.4.1.R02; support for binding L2 GRE tunnel services to unicast SDPs added.

Related Commands

- `service sdp vxlan`: Manually configures a VXLAN SDP (multicast or unicast)
- `service sdp l2gre`: Manually configures an L2 GRE unicast SDP.
- `service vxlan`: Configures a VXLAN service.
- `service l2gre`: Configures an L2 GRE tunneling service.
- `show service sdp`: Displays the SDP configuration for the switch.
- `show service bind-sdp`: Displays the service-to-SDP binding configuration for the switch.
MIB Objects

alaSdpBindTable
  alaSdpBindId
  alaSdpBindCreationOrigin
  alaSdpBindSvcType
  alaSdpBindAdminStatus
  alaSdpBindStatsAdminStatus
  alaSdpBindMode
  alaSdpBindFarEndIpAddress
  alaSdpBindVnid
  alaSdpBindDescription
  alaSdpBindRowStatus
**service l2gre auto-discover**

Configures the status of L2 GRE automatic SDP discovery on a tunnel aggregation switch. When enabled, the switch discovers the SDPs of remote tunnel end points for a configured L2 GRE service. Once discovered, the switch will dynamically create local SDP and SDP bindings for the remote tunnel end points of the L2 GRE service.

```
service l2gre auto-discover {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables automatic discovery of L2 GRE edge switches.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables automatic discovery of L2 GRE edge switches.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, automatic discovery is enabled on an L2 GRE tunnel aggregation switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When L2 GRE automatic discovery is enabled (the default), the detection of SDPs for remote tunnel end points is based on the traffic received from these end points. If the destination IP address of the remote traffic is the IP address of the local Loopback0 interface and the VPNID of the traffic matches the VPNID of a local L2 GRE service, an SDP and SDP binding is dynamically created for the remote tunnel end point.

- When L2 GRE automatic discovery is disabled, manual configuration of an SDP and SDP binding for a remote tunnel end point is required using the `service sdp l2gre` and `service sdp-bind` commands.

- L2 GRE automatic discovery on the tunnel aggregation switch is similar to how tunnel access switches automatically define unicast SDPs to the aggregation switch.

- Configuring L2 GRE tunneling on an OmniSwitch 6900-T20/T40 or OmniSwitch 6900-X20/X40 is recommended when these models are part of a mixed VC and the L2 GRE SDP is configured on one of the other switches in the mixed VC (for example, on an OmniSwitch 6900-X72/Q32 or OmniSwitch 6900-V72/C32). This ensures that all routing and multicast functionality required to support an L2 GRE tunnel service is limited to a switch that supports SDP configuration.

**Examples**

```
-> service l2gre auto-discover disable
-> service l2gre auto-discover enable
```
Release History

Release 8.5R2; command was introduced.

Related Commands

- service sdp l2gre
  Configures an SDP for L2 GRE tunnel traffic.
- service bind-sdp
  Configures the binding of an L2 GRE tunnel service to an SDP
- show service info
  Displays the Service Manager configuration for the local switch.

MIB Objects

alaSvcMgrSysTable
  alaSvcMgrSdpAutoCreateAdminState
service rfp local-endpoint

Configures a local end point for an SPB Remote Fault Propagation (RFP) domain. Creating a local RFP end point identifies the local switch as a Maintenance End Point (MEP) in the RFP domain.

service rfp rfp_id local-endpoint lep_id [admin-state {enable | disable}] [ccm-interval {interval100ms | interval1s | interval10s | interval1m | interval10m | interval-invalid}] [level number] type spb

no service rfp rfp_id [local-endpoint lep_id]

Syntax Definitions

rfp_id  A unique numerical value to identify an RFP domain that maps to a reserved OAM domain. The valid RFP ID range is 1–32767.

lep_id  A numerical value to identify an end point of the specified RFP domain ID on the local switch. The valid range is 1–8191. This value serves as the virtual UP MEP ID for the RFP end point.

enable  Administratively enables the local end point.

disable  Administratively disables the local end point.

interval100ms  Send a Continuity Check Messages (CCM) every 100 milliseconds.

interval1s  Send a CCM every 1 second.

interval10s  Send a CCM every 10 seconds.

interval1m  Send a CCM every minute.

interval10m  Send a CCM every 10 minutes.

interval-invalid  Send a CCM by a MEP.

number  A unique numerical value to assign as the OAM domain level for the RFP domain. The valid range is 0-7.

Defaults

When a local end point is created for an RFP domain without specifying any of the optional parameter values, the end point is created with the following default values:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>ccm-interval</td>
<td>interval1s</td>
</tr>
<tr>
<td>number</td>
<td>7</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to remove the RFP domain configuration from the switch (for example, `no service rfp 1`). To remove the local end point ID only, use the `no` form of this command with the `local-endpoint` parameter (for example, `no service rfp local-endpoint`).

- An RFP domain consists of a local end point configured with this command and a remote end point list configured with the `service rfp remote-endpoint` command. An SPB service is bound to the remote end point list to identify the Service Access Point (SAP) to monitor.

- The local end point ID number identifies local BEB devices in the RFP domain; this is also the number used as the virtual UP MEP ID.

- Creating more than one RFP domain with the same domain level value is not allowed. Up to eight RFP domains are allowed as long as they each are created with a different level number. Each RFP domain created counts towards the maximum limit of Ethernet OAM domains allowed.

- When this command is used to create an RFP end point, the switch automatically creates the following reserved Ethernet OAM elements that are mapped to each RFP domain:
  - Maintenance Domain (MD) named “RFP_OVER_SPB_DOMAIN_LEVEL7”, where the level number is the value specified with this command. Each time an RFP end point is created, a new maintenance domain is created with the level number specified with this command.
  - Maintenance Association (MA) named “RFP_OVER_SPB_ASSOCIATION”. The same MA name is used for all RFP domains.
  - A primary VLAN, where the VLAN ID used is the SPB control BVLAN. This same VLAN is used as the primary VLAN for all RFP domains.
  - Virtual UP Maintenance End Point (MEP) that will advertise CCM to the network. Each CCM contains a proprietary OUI TLV that specifies I-SID information and the state of the port associated with the I-SID. CCM packets are sent using the CCM interval value specified with this command. The local end point ID specified with this command serves as the virtual UP MEP ID.

Examples

- `-> service rfp 1000 local-endpoint 1 ccm-interval INTERVAL1s type SPB`
- `-> service rfp 1000 local-endpoint 1 admin-status enable`
- `-> service rfp 2000 local-endpoint 1 admin-status enable ccm-interval INTERVAL1s level 6 type SPB`
- `-> service rfp 300 local-endpoint 40 ccm-interval INTERVAL1s type level 5 SPB`
- `-> service rfp 300 local-endpoint 40 admin-status enable`
- `-> no service rfp 1 local-endpoint 1000`

Release History

Release 7.3.4; command was introduced.
Related Commands

**service rfp remote-endpoint**  Configures a remote end point that is associated with the local end point through the RFP ID.

**show service rfp**  Displays the configuration and status of RFP for SPB domains.

**show service rfp configuration**  Displays the RFP OAM domain configuration for the bridge.

MIB Objects

alaRfpSpbLocalEndPointTable
  alaRfpSpbLocalEndPointRfp
  alaRfpSpbLocalEndPoint
  alaRfpSpbLocalEndPointCcmInterval
  alaRfpSpbLocalEndPointAdminStatus
  alaRfpSpbLocalEndPointLevel
  alaRfpSpbLocalEndPointCBVlan
  alaRfpSpbLocalEndPointMaintDomain
  alaRfpSpbLocalEndPointMaintAssociation
**service rfp remote-endpoint**

Configures a remote end point list for an SPB Remote Fault Propagation (RFP) domain. The list consists of the MEP IDs on remote BEBs and local SPB service ID numbers. This command triggers the sending of a Continuity Check Message (CCM) to advertise the status of the specified local SPB services to the specified remote MEP IDs.

```
service rfp rfp_id remote-endpoint rep_id service-id [service_id[[-service_id2]]
```

```
no service rfp rfp_id remote-endpoint rep_id [service-id [service_id[[-service_id2]]]
```

### Syntax Definitions

- **rfp_id**: An existing RFP ID number.
- **rep_id**: A numerical value to identify the MEP ID of a remote BEB. The valid range is 1–8191.
- **service_id[[-service_id2]]**: An existing SPB service ID to bind to the RFP domain. Use a hyphen to specify a range of SPB services (for example, 10-12 specifies services 10, 11, and 12).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the RFP end point or an SPB service ID from the end point list.
- To identify a BEB as a participating member of an RFP domain, first configure a local RFP end point with the `service rfp local-endpoint` command to create the RFP domain ID then use this command to configure the remote end point. Both types of end points use the same RFP ID, but the RFP ID specified for the remote end point must already exist.
- The MEP ID specified with this command is the end-point ID configured on the remote BEB using the `service rfp local-endpoint` command.
- One or more SPB services are bound to the RFP remote end point to identify the Service Access Point (SAP) to monitor within the RFP domain. An SPB service is associated with an SPB service instance ID (I-SID); the service is then associated with a SAP. A SAP binds together the service and the access port on which device traffic enters the SPB service domain.
Each SPB service bound to an RFP domain identifies the SAP information (such as access port status and I-SID) that is advertised in the proprietary TLV of CCM packets. Each CCM may contain information for multiple SPB services.

Although binding multiple SPB services to an RFP domain is allowed, monitoring SAPs associated with only one SPB service is recommended.

**Examples**

```
-> service rfp 1000 remote-endpoint 2 service-id 10-14
-> service rfp 1000 remote-endpoint 3 service-id 20
-> no service rfp 1000 remote-endpoint 2 service-id 10
-> no service rfp 1000 remote-endpoint 2
-> no service rfp 1000
```

Example when the RFP ID does not exist because a local end point with that ID was not created:

```
-> service rfp 2000 remote-endpoint 2 service-id 10
ERROR: RFP Domain (2000) does not exist
```

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `service rfp local-endpoint` Configures a local end point that is associated with the remote end point through the RFP ID.
- `show service rfp` Displays the configuration and status of RFP for SPB domains.
- `show service rfp configuration` Displays the RFP OAM domain configuration for the bridge.

**MIB Objects**

- `alaRfpSpbRemoteEndPointTable` contains the remote end point table
- `alaRfpSpbRemoteEndPointRfp`
- `alaRfpSpbRemoteEndPoint`
- `alaRfpSpbRemoteEndPointServiceID`
- `alaRfpSpbRemoteEndPointStatus`
- `alaRfpSpbRemoteEndPointSystemName`
- `alaRfpSpbRemoteEndPointISID`
- `alaRfpSpbRemoteEndPointBVlan`
show service l2profile

 Displays the Layer 2 profile configuration information for the bridge. This type of profile is applied to access (customer-facing) ports and specifies how to process Layer 2 protocol frames received on this type of port.

 show service l2profile [profile_name]

 Syntax Definitions

 profile_name

 An existing Layer 2 profile name. Use quotes around string if the profile name contains multiple words with spaces between them (for example, “ALE Engineering”).

 Defaults

 By default, all profiles are displayed if a profile name is not specified with this command.

 Platforms Supported

 This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td>X48C6/T48C6/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C6/E/V48C8/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

 Usage Guidelines

 • Use the profile-name parameter to display information for a specific profile. Entering a profile name is case sensitive.

 • If there are no profiles configured for the switch, this command will still display the information for the default profiles (def-access-profile, pw-def-access-profile, and unp-def-access-profile).
   – The def-access-profile is applied to service access ports that are not associated with a specific profile.
   – The pw-def-access-profile replaces the def-access-profile when the access port is assigned to an SPB pseudo-wire SAP.
   – The unp-def-access-profile is applied to UNP access ports.

 • An asterisk (*) appears after a profile name when the profile is assigned to UNP access ports.

 Examples

 -> show service l2profile

 Legend: (*) in-use by UNP

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>STP</th>
<th>802.1X</th>
<th>802.3AD</th>
<th>MVRP</th>
<th>GVRP</th>
<th>AMAP</th>
<th>Both</th>
<th>Tagged</th>
<th>Untagged</th>
</tr>
</thead>
<tbody>
<tr>
<td>def-access-profile</td>
<td>tunnel</td>
<td>drop</td>
<td>peer</td>
<td>tunnel</td>
<td>tunnel</td>
<td>drop</td>
<td>drop</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>DropL2</td>
<td>drop</td>
<td>drop</td>
<td>drop</td>
<td>tunnel</td>
<td>drop</td>
<td>drop</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>lldp-tag-untag</td>
<td>tunnel</td>
<td>drop</td>
<td>peer</td>
<td>tunnel</td>
<td>tunnel</td>
<td>drop</td>
<td>-</td>
<td>-</td>
<td>tunnel</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide    April 2023
Service Manager Commands

show service l2profile

ldp-tunnel         tunnel  drop  peer  tunnel  tunnel  drop  tunnel  -  -
pw-def-access-profile tunnel  tunnel  peer  tunnel  tunnel  tunnel  tunnel
unp-def-access-profile drop  peer  peer  tunnel  tunnel  drop  drop  -  -

-> show service l2profile DropL2

Legend: (*) in-use by UNP

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>STP</th>
<th>802.1x</th>
<th>802.3AD</th>
<th>MVRP</th>
<th>GVRP</th>
<th>AMAP</th>
<th>Both</th>
<th>Tagged</th>
<th>Untagged</th>
</tr>
</thead>
<tbody>
<tr>
<td>DropL2</td>
<td>drop</td>
<td>drop</td>
<td>drop</td>
<td>tunnel</td>
<td>drop</td>
<td>drop</td>
<td>drop</td>
<td>drop</td>
<td>-</td>
</tr>
</tbody>
</table>

output definitions

**Profile Name**
The name of the Layer 2 profile.

**Stp**
Indicates how Spanning Tree traffic control packets are processed.

**802.1x**
Indicates how IEEE 802.1x control packets are processed.

**802.3ad**
Indicates how IEEE 802.3ad control packets are processed.

**MVRP**
Indicates how Multiple VLAN Registration Protocol packets are processed.

**GVRP**
Indicates how GARP VLAN Registration Protocol packets are processed.

**AMAP**
Indicates how Alcatel-Lucent Enterprise Mapping Adjacency Protocol packets are processed.

**802.1AB Both**
Indicates how tagged and untagged IEEE 802.1AB control packets are processed.

**802.1AB Tagged**
Indicates how tagged IEEE 802.1AB control packets are processed.

**802.1AB Untagged**
Indicates how untagged IEEE 802.1AB control packets are processed.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN service support added.
Release 8.4.1; Layer 2 profiles for UNP access ports included in the output display.
Release 8.4.1.R02; L2 GRE tunnel service support added.
Release 8.6R2; “802.1AB Both”, “802.1AB Tagged”, and “802.1AB Untagged” fields added.
Release 8.7R2; Layer 2 profile **pw-def-access-profile** for SPB pseudo-wire access ports included in the output display.

Related Commands

- **service l2profile**
  Configures a Layer 2 profile that is applied to a service access port.

- **service l2profile inbound 802.1ab**
  Configures how tagged and untagged 802.1AB control frames are processed.

- **service access l2profile**
  Assigns an existing Layer 2 profile to the specified service access port

- **unp l2-profile**
  Assigns an existing Layer 2 profile to the specified UNP access port

- **show service access**
  Displays the access (customer-facing) port configuration for the bridge.
**MIB Objects**

alaServiceMgrPortProfileTable
alaServiceMgrPortProfileID
alaServiceMgrPortProfileStpBpduTreatment
alaServiceMgrPortProfile8021xTreatment
alaServiceMgrPortProfile8021ABTreatment
alaServiceMgrPortProfileGvrpTreatment
alaServiceMgrPortProfileAmapTreatment
alaServiceMgrPortProfile8023ADTreatment
alaServiceMgrPortProfile8021ABTagTreatment
alaServiceMgrPortProfile8021ABUnTagTreatment
alaServiceMgrPortProfile8021ABMode
show service access

Displays the access (customer-facing) port configuration for the bridge.

`show service access [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] | sap]`

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **sap**
  - Displays the Service Access Points (SAPs) associated with the specified access port.

**Defaults**

By default, all service access ports are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `port` and `linkagg` parameters to display the configuration for a specific port or link aggregate.
- Use the `sap` parameter to display the SAPs associated with the specified port.

**Examples**

```
-> show service access
Port   Link   SAP   SAP   Vlan
Id     Status  Type  Count Xlation L2Profile              Description
-------+--------+-------+------+=---------------+----------------------------------
1/1/11  Up     Manual 100   N   def-access-profile
1/1/12  Up     Manual 100   N   def-access-profile
1/1/13  Down   Dynamic 100   N   unp-def-access-profile UNP Dynamic Access Port
1/1/14  Down   Manual 100   N   pw-def-access-profile

Total Access Ports: 4
```
-> show service access port 1/1/13
Port     Link  SAP     SAP   Vlan
Id       Status Type  Count Xlation L2Profile    Description
-------+------+-------+-=---+-------+------------------+-----------------------
1/1/13  Down   Dynamic 100   N       unp-def-access-profile UNP Dynamic Access Port
Total Access Ports: 1

output definitions
Port Id: The access port number or link aggregate ID number.
Link Status: The status of the link connection to the access port (Up or Down).
SAP Type: Whether or not the SAP associated with the access port was created statically or dynamically (Manual or Dynamic).
SAP Count: The number of service access points (SAPs) that are associated with the access port.
VLAN Xlation: Whether or not VLAN translation is enabled on the access port.
L2Profile: The name of the Layer 2 profile associated with the access port. Configured through the service l2profile command.
Description: An optional description configured for the access port. By default, the description is blank.

-> show service access port 1/1/23 sap
Legend: * denotes a dynamic object
Identifier       Adm  Oper Stats T:P  ServiceId   Isid/Vnid Xlation Sap Description
----------------+----+----+-----+----+-----------+---------+-------+---------------
sap:1/1/23:0     Down Down  N    Y:x  20          1500        N      -
sap:1/1/23:all   Up   Down  N    N:3  10          2300        N      VXLAN SAP
sap:1/1/23:9.10  Down Down  N    Y:x  20           200        N      L2GRE SAP
Total SAPs: 3

output definitions
Identifier: The SAP identifier, which consists of the access port and encapsulation value.
Adm: The administrative state of the SAP (Up or Down).
Oper: The operational state of the SAP (Up or Down).
Stats: Whether or not statistics collection is enabled for the SAP (Yes or No).
T:P: Whether or not the 802.1p priority value of traffic mapped to this SAP is trusted. (Y or N). If this value is set to untrusted (N), then the traffic is marked with the specified 802.1p priority value. For example, Y:x indicates traffic priority is trusted; N:3 indicates traffic priority is untrusted and should be marked with an 802.1p value of 3.
ServiceId: The ID number of the service associated with the SAP.
Isid/Vnid: An SPB service instance identifier (ISID), VXLAN network identifier (VNID), or an L2 GRE Virtual Private Network (VPN) identifier. The value of this field depends on whether an SPB service, a VXLAN service, or an L2 GRE tunnel service is associated with the SAP.
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan Translation</td>
<td>Whether or not VLAN translation is enabled for the SAP (Yes or No).</td>
</tr>
<tr>
<td>Sap Description</td>
<td>An optional description configured for the SAP. By default, the description is blank.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; description field added.
Release 7.3.4; sap parameter added; VXLAN service support added.
Release 8.4.1.R02; L2 GRE tunnel service support added.

Related Commands

service access Configures a switch port or link aggregate as a service access port.
show service l2profile Displays the Layer 2 profile configuration for the bridge.

MIB Objects

alaServiceMgrPortTable
  alaServiceMgrPortID
  alaServiceMgrPortMode
  alaServiceMgrPortPortProfileID
  alaServiceMgrPortLinkStatus
  alaServiceMgrPortSapType
  alaServiceMgrPortSapCount
  alaServiceMgrPortVlanXlation
  alaServiceMgrPortDescription
show service

Displays information about the services configured on the switch.

show service [spb | vxlan | l2gre | service_id [sap tcp-mss]]

Syntax Definitions

spb Displays only the Shortest Path Bridging (SPB) services.
vxlan Displays only the Virtual eXtensible LAN (VXLAN) services.
l2gre Displays only the Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services.

service_id An existing service ID number. Displays additional details about the specified service.
sap tcp-mss Displays the TCP Maximum Segment Size (TCP-MSS) configuration.

Defaults

By default, a list of all services is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>L2 Gre</th>
<th>VXLAN</th>
<th>SPB</th>
<th>TCP-MSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570N</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C8/C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the spb parameter to display additional information about SPB services.
- Use the vxlan parameter to display additional information about VXLAN services.
- Use the l2gre parameter to display additional information about L2 GRE tunnel services.
- The service ID is a unique number that identifies a specific service. Information associated with the service ID is displayed.

Examples

-> show service
Legend: * denotes a dynamic object
All Service Info
Svc            SAP   Bind
ServiceId     Type  Adm  Oper Stats Count Count Description
-----------------------------------------------
1             VxLAN Up   Up    Y    1     3     VXLAN Svc VNID 1000
2             VxLAN Up   Up    N    1     1     VXLAN Svc VNID 2000
3           VxLAN Up   Down  Y    0     0     VXLAN Svc VNID 3000
50          L2GRE Up   Down  N    0     0     L2 GRE Tunnel
100         SPB   Up   Up    Y    2     2     SPB Svc ISID 1000
200         SPB   Down Down  N    0     0     SPB Svc ISID 2000
250         L2GRE Up   Up    Y    1     1     L2GRE Svc VPNID 251
32768*      SPB   Up   Up    Y    1     1     UNP Dynamic Svc ISID 4000
32769*      VxLAN Up   Up    Y    1     3     UNP Dynamic Svc VNID 5000
32770*      L2GRE Up   Up    Y    0     1     Dynamic Service vpnid=100 for UNP

Total Services: 9

output definitions

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>The service ID number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Svc Type</td>
<td>The type of service (SPB, VXLAN, or L2GRE).</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the service (Up or Down).</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the service (Up or Down).</td>
</tr>
<tr>
<td>Stats</td>
<td>Whether or not statistics collection is enabled for the service.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of Service Access Points (SAPs) associated with this service.</td>
</tr>
<tr>
<td>Bind Count</td>
<td>The number of Service Distribution Points (SDPs) bound to this service.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description configured for the service.</td>
</tr>
</tbody>
</table>

-> show service spb
Legend: * denotes a dynamic object
SPB Service Info
   SystemId : 00e0.b1e7.0188,   SrcId : 0x70188,    SystemName : TOR-1

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>SAP Count</th>
<th>Bind Count</th>
<th>Isid</th>
<th>BVlan</th>
<th>Mode</th>
<th>(T/R)</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Up</td>
<td>Down</td>
<td>Y</td>
<td>8</td>
<td>4</td>
<td>1000</td>
<td>4001</td>
<td>Headend</td>
<td>(0/0)</td>
</tr>
<tr>
<td>200</td>
<td>Down</td>
<td>Down</td>
<td>N</td>
<td>0</td>
<td>0</td>
<td>1001</td>
<td>4001</td>
<td>Headend</td>
<td>(0/0)</td>
</tr>
<tr>
<td>32768*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>23</td>
<td>4</td>
<td>1002</td>
<td>4001</td>
<td>Headend</td>
<td>(0/0)</td>
</tr>
</tbody>
</table>

Total Services: 3

output definitions

<table>
<thead>
<tr>
<th>SystemId</th>
<th>The MAC address of the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcId</td>
<td>The Source ID value.</td>
</tr>
<tr>
<td>System Name</td>
<td>The name assigned to the switch.</td>
</tr>
<tr>
<td>ServiceId</td>
<td>The service ID number.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the service (Up or Down).</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the service (Up or Down).</td>
</tr>
<tr>
<td>Stats</td>
<td>Whether or not statistics collection is enabled for the service.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of Service Access Points (SAPs) associated with this SPB service.</td>
</tr>
<tr>
<td>Bind Count</td>
<td>The number of Service Distribution Points (SDPs) bound to this SPB service.</td>
</tr>
</tbody>
</table>
output definitions

- **Isid**: The service instance identifier that identifies the SPB service instance within the provider backbone bridging (PBB) network. This field is displayed only for SPB services.

- **BVlan**: The VLAN ID number for the backbone VLAN to which the SPB service is mapped. This field is displayed only for SPB services.

- **MCast Mode**: The multicast replication mode (Headend, Tandem, or Hybrid) for the service.

- **T/R**: The number of packets transmitted and received for this service. This field is displayed only for SPB services.

---

```
show service vxlan
Legend: * denotes a dynamic object
VxLAN Service Info

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>SAP Count</th>
<th>Bind Count</th>
<th>Vnid</th>
<th>VndId</th>
<th>VndType</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>1</td>
<td>3</td>
<td>1000 (0.1.56)</td>
<td>224.2.1.1</td>
<td>Tandem</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>2</td>
<td>1</td>
<td>2000 (0.7.208)</td>
<td></td>
<td></td>
<td>Headend</td>
</tr>
<tr>
<td>3</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>2</td>
<td>1</td>
<td>3000 (0.11.184)</td>
<td></td>
<td></td>
<td>Headend</td>
</tr>
<tr>
<td>32769*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>1</td>
<td>3</td>
<td>5000 (0.19.136)</td>
<td>225.1.1.1</td>
<td>Tandem</td>
<td></td>
</tr>
</tbody>
</table>

Total Services: 4
```

output definitions

- **ServiceId**: The service ID number.

- **Adm**: The administrative state of the service (Up or Down).

- **Oper**: The operational state of the service (Up or Down).

- **Stats**: Whether or not statistics collection is enabled for the service.

- **SAP Count**: The number of Service Access Points (SAPs) associated with this VXLAN service.

- **Bind Count**: The number of Service Distribution Points (SDPs) bound to this VXLAN service.

- **Vnid**: The VXLAN network identifier (VNID) that identifies a VXLAN segment. The decimal notation format of the VNID is also included (for example, VNID 1000 is also represented as 0.1.56).

- **MCast Mode**: The multicast replication mode (Headend, Tandem, or Hybrid) for the service.

---

```
show service l2gre
Legend: * denotes a dynamic object
L2GRE Service Info

<table>
<thead>
<tr>
<th>ServiceId</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>SAP Count</th>
<th>Bind Count</th>
<th>Vpid</th>
</tr>
</thead>
<tbody>
<tr>
<td>50</td>
<td>Up</td>
<td>Down</td>
<td>N</td>
<td>0</td>
<td>0</td>
<td>24000</td>
</tr>
<tr>
<td>250</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>1</td>
<td>1</td>
<td>251</td>
</tr>
<tr>
<td>32770*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>0</td>
<td>1</td>
<td>100</td>
</tr>
</tbody>
</table>
```
Total Services: 2

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServiceId</td>
<td>The service ID number.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the service (Up or Down).</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the service (Up or Down).</td>
</tr>
<tr>
<td>Stats</td>
<td>Whether or not statistics collection is enabled for the service.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of Service Access Points (SAPs) associated with this L2 GRE tunnel service.</td>
</tr>
<tr>
<td>Bind Count</td>
<td>The number of Service Distribution Points (SDPs) bound to this L2 GRE tunnel service.</td>
</tr>
<tr>
<td>Vpnid</td>
<td>A GRE tunnel Virtual Private Network (VPN) ID.</td>
</tr>
</tbody>
</table>

-> show service 100

```
SPB Service Detailed Info
Service Id       : 100,                  Description      : SPB Svc ISID 1000,
ISID             : 1000,                 BVlan            : 4001,
Multicast-Mode   : Headend,              Tx/Rx Bits       : 0/0,
Admin Status     : Up,                   Oper Status      : Down,
Stats Status     : Yes,                  Vlan Translation : No,
Service Type     : SPB,                  Allocation Type  : Static,
MTU              : 9194,                 VPN IP-MTU       : 1500,
SAP Count        : 8,                    SDP Bind Count   : 4,
RemoveIngressTag : No,                  Option           : None,
IPv4 VRF Instance: Default,             IPv4 Interface   : l3vpn-100,
IPv6 VRF Instance: Default,             IPv6 Interface   : l3vpn-100,
Ingress Pkts     : 0,                    Ingress Bytes    : 0,
Egress Pkts      : 0,                    Egress Bytes     : 0,
```

-> show service 120

```
SPB Service Detailed Info
Service Id       : 120,                 Description      : Pseudo-wire ISID 1001,
ISID             : 1001,                BVlan            : 4000,
Multicast-Mode   : Headend,              Tx/Rx Bits       : 0/0,
Admin Status     : Up,                   Oper Status      : Up,
Stats Status     : No,                   Vlan Translation : No,
Service Type     : SPB,                  Allocation Type  : Static,
MTU              : 9194,                 VPN IP-MTU       : 1500,
SAP Count        : 1,                    SDP Bind Count   : 1,
RemoveIngressTag : No,                  Option           : Pseudo-wire,
Mgmt Change      : 12/05/2015 18:42:43,  Status Change    : 12/05/2015 18:42:43
```

-> show service 1

```
VxLAN Service Detailed Info
Service Id       : 1,                    Description      : VXLAN Svc VNID 1000,
VNID             : 1000 (0.1.56),         Multicast-Mode   : Tandem,
Admin Status     : Up,                   Oper Status      : Up,
Stats Status     : Yes,                  Vlan Translation : No,
Service Type     : VxLAN,                Allocation Type  : Static,
MTU              : 9194,                 VPN IP-MTU       : 1500,
SAP Count        : 1,                    SDP Bind Count   : 3,
RemoveIngressTag : No,                  Ingress Bytes    : 0,
Ingress Pkts     : 0,                    Egress Bytes     : 0,
```
Egress Pkts     : 0,     Egress Bytes  : 0,  
Mgmt Change    : 10/19/2014 13:20:42,  Status Change : 10/19/2014 13:20:42->
show service 50
L2GRE Service Detailed Info
<table>
<thead>
<tr>
<th>Service Id</th>
<th>50,</th>
<th>Description</th>
<th>L2 GRE Tunnel,</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPNID</td>
<td>24000,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Status</td>
<td>Up,</td>
<td>Oper Status</td>
<td>Down,</td>
</tr>
<tr>
<td>Stats Status</td>
<td>No,</td>
<td>Vlan Translation</td>
<td>No,</td>
</tr>
<tr>
<td>Service Type</td>
<td>L2GRE,</td>
<td>Allocation Type</td>
<td>Static,</td>
</tr>
<tr>
<td>MTU</td>
<td>9194,</td>
<td>VPN IP-MTU</td>
<td>1500,</td>
</tr>
<tr>
<td>SAP Count</td>
<td>0,</td>
<td>SDP Bind Count</td>
<td>0,</td>
</tr>
<tr>
<td>RemoveIngressTag</td>
<td>No,</td>
<td>Port Isolation</td>
<td>Enable,</td>
</tr>
<tr>
<td>Ingress Pkts</td>
<td>0,</td>
<td>Ingress Bytes</td>
<td>0,</td>
</tr>
<tr>
<td>Egress Pkts</td>
<td>0,</td>
<td>Egress Bytes</td>
<td>0,</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Service Id</th>
<th>The service identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>An optional description configured for the service. By default, the description is blank.</td>
</tr>
<tr>
<td>ISID</td>
<td>The service instance identifier (I-SID) number for the SPB service. This field is only displayed for SPB services.</td>
</tr>
<tr>
<td>BVlan</td>
<td>The VLAN ID number for the SPB backbone VLAN (BVLAN). This field is only displayed for SPB services.</td>
</tr>
<tr>
<td>VNID</td>
<td>The VXLAN network identifier for the VXLAN segment. This field is only displayed for VXLAN services.</td>
</tr>
<tr>
<td>VPNID</td>
<td>A GRE tunnel Virtual Private Network (VPN) ID. This field is only displayed for L2 GRE tunnel services.</td>
</tr>
<tr>
<td>Multicast-Mode</td>
<td>The multicast replication mode for the specified service (<strong>tandem</strong>, <strong>headend</strong>, or <strong>hybrid</strong>). This field is not displayed for L2 GRE tunnel services.</td>
</tr>
<tr>
<td>Tx/Rx Bits</td>
<td>The number of bits transmitted and received for this service. This field is only displayed for SPB services.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The administrative state of the service (<strong>Up</strong> or <strong>Down</strong>).</td>
</tr>
<tr>
<td>Oper Status</td>
<td>The operational state of the service (<strong>Up</strong> or <strong>Down</strong>).</td>
</tr>
<tr>
<td>Stats Status</td>
<td>Whether statistics collection is enabled for the service (<strong>Yes</strong> or <strong>No</strong>).</td>
</tr>
<tr>
<td>Vlan Translation</td>
<td>Whether VLAN translation is enabled for the service (<strong>Yes</strong> or <strong>No</strong>).</td>
</tr>
<tr>
<td>Service Type</td>
<td>The type of service (<strong>SPB</strong>, <strong>VXLAN</strong>, or <strong>L2GRE</strong>).</td>
</tr>
<tr>
<td>Allocation Type</td>
<td>Whether the service was manually or dynamically created (<strong>Static</strong> or <strong>Dynamic</strong>).</td>
</tr>
<tr>
<td>MTU</td>
<td>The largest frame size, in octets, that the service can handle.</td>
</tr>
<tr>
<td>SAP Count</td>
<td>The number of SAPs associated with this service.</td>
</tr>
<tr>
<td>SDP Bind Count</td>
<td>The number of SDPs bound to this service.</td>
</tr>
<tr>
<td>RemoveIngressTag</td>
<td>Whether the customer VLAN tag is removed before the packet is encapsulated for the service (<strong>Yes</strong> or <strong>No</strong>).</td>
</tr>
</tbody>
</table>
Service Manager Commands

Related Commands

- **service spb**
  - Configures an SPB service.

- **service pseudo-wire**
  - Configures an SPB service to operate as a point-to-point (E-LINE) service.

- **service vxlan**
  - Configures a VXLAN service.

- **service l2gre**
  - Configures an L2 GRE tunnel service.

- **show service ports**
  - Displays the virtual ports (SAPs, SDPs) associated with the service.

- **show service sdp**
  - Displays the SDP configuration for the bridge.

- **show service bind-sdp**
  - Displays the Mesh SDP bindings for the bridge.

Release History

- Release 7.3.1; command was introduced.
- Release 7.3.4; **vxlan** parameter added.
- Release 8.4.1.R02; **l2gre** parameter added.
- Release 8.6R1; “Port Isolation” field added for L2 GRE tunnel services.
- Release 8.7R2; “Pseudo-wire” added to “Option” field for SPB services.

Option

- **Option**
  - The type of tunnel endpoint defined by the service (**pseudo-wire** or **None**). A pseudo-wire endpoint is configured to define a point-to-point connection that will provide a transparent E-LINE service. If this option is set to **None**, the service is operating in the default mode, where tunnel endpoints are automatically defined between all the SPB nodes with the same backbone service instance (I-SID).

IPv4 VRF Instance
IPv6 VRF Instance

- **IPv4 VRF Instance**
  - The name of the VRF instance in which an IP interface that is bound to the SPB service is configured. This field is displayed only when the SPB service is associated with an L3 VPN IP interface.

- **IPv6 VRF Instance**
  - The name of the VRF instance in which an IP interface that is bound to the SPB service is configured. This field is displayed only when the SPB service is associated with an L3 VPN IP interface.

IPv4 Interface
IPv6 Interface

- **IPv4 Interface**
  - The name of the IP interface that is bound to the SPB service. This field is displayed only when the SPB service is associate with an L3 VPN IP interface.

- **IPv6 Interface**
  - The name of the IP interface that is bound to the SPB service. This field is displayed only when the SPB service is associate with an L3 VPN IP interface.

Port Isolation

- **Port Isolation**
  - The status of port isolation for an L2 GRE tunnel service. When enabled, traffic between L2 GRE tunnel SAPs is dropped. Port isolation is implicitly enabled and is not configurable in this release.

Ingress Pkts
Ingress Bytes
Egress Pkts
Egress Bytes
Mgmt Change
Status Change

- **Ingress Pkts**
  - The number of packets that have ingressed on this SAP.

- **Ingress Bytes**
  - The number of bytes that have ingressed on this service.

- **Egress Pkts**
  - The number of packets that have egressed on this service.

- **Egress Bytes**
  - The number of bytes that have egressed on this service.

- **Mgmt Change**
  - The date and time of the last configuration change for this service.

- **Status Change**
  - The date and time of the last operational status change for this service.
MIB Objects

alaSvcBaseInfoTable
  alaSvcId
  alaSvcType
  alaSvcDescription
  alaSvcMtu
  alaSvcAdminStatus
  alaSvcOperStatus
  alaSvcNumSaps
  alaSvcNumSdp
  alaSvcLastMgmtChange
  alaSvcLastStatusChange
  alaSvcAllocationType
  alaSvcStatsAdminStatus
  alaSvcIsid
  alaSvcBvlan
  alaSvcMulticastMode
  alaSvcIngressPacketCount
  alaSvcIngressByteCount
  alaSvcEgressPacketCount
  alaSvcEgressByteCount
  alaSvcSapVlanXlation
  alaSvcVnid
  alaSvcRemoveIngressTag
  alaSvcL3VpnIfName
  alaSvcL3VpnVrfName
  alaSvcVpnId
  alaSvcOption
  alaSvcRemoteSystemId
show service ports

Displays the virtual ports associated with the specified Shortest Path Bridging (SPB) service, Virtual eXtensible LAN (VXLAN) service, or Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel service.

`show service {service_id | isid instance_id | vnid vxlan_id | vpnid vpn_id} ports`

Syntax Definitions

- **service_id**: An existing service ID number.
- **instance_id**: Displays the virtual ports associated with the specified SPB service instance identifier (I-SID) number. The valid range is 256–16777214.
- **vxlan_id**: Displays the virtual ports associated with the specified VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).
- **vpn_id**: Displays the virtual ports associated with the specified L2 GRE tunnel Virtual Private Network (VPN) ID.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- A Service Access Point (SAP) and a Service Distribution Point (SDP) serve as virtual ports that carry traffic for the specified SPB service, VXLAN service, or L2 GRE tunnel service.
- In addition to the virtual port configuration, this command also provides the status and additional configuration information for the SPB service, VXLAN service, or L2 GRE tunnel service.

Examples

`-> show service 525 ports`

Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object

SPB Service 525 Info


<table>
<thead>
<tr>
<th>Sap Trusted:Priority/</th>
<th>Sap Description /</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier Adm Oper Stats Sdp SystemId:BVlan Intf Sdp SystemName</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
Service Manager Commands

```
sap:1/1/11:2524  Up  Up  N       Y:x     1/1/11  -
sap:1/1/12:2524  Up  Up  N       Y:x     1/1/12  -
sap:1/1/13:2524  Up  Down  N      Y:x     1/1/13  -
sap:1/1/14:2524  Up  Down  N      Y:x     1/1/14  -
sdp:32806:525*   Up  Up  Y       e8e7.3233.1831:4004 1/1/1  BRIDGE-4
```

Total Ports: 5

```
-> show service 20 ports
Legend: (*)Dyn unicast (+)Remote Mcast (#)Local Mcast (-)ERP Ring
SPB Service 20 Info
 Admin : Up,  Oper : Down, Stats : Y,  Mtu : 9194, VlanXlation : N,
 ISID : 1501, BVlan : 4000, MCast-Mode : Headend, Tx/Rx : 0/0, RemoveIngTag: N,
 PW-Enb: Y,

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp SystemId:BVlan</th>
<th>Intf</th>
<th>Sdp SystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/5:all</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>Y:x</td>
<td>1/1/5</td>
<td>-</td>
</tr>
<tr>
<td>sdp:32768:100*</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>e8e7.32f8.5b41:4000</td>
<td>0/120</td>
<td>X72_VC</td>
</tr>
</tbody>
</table>
```

Total Ports: 2

```
-> show service isid 1500 ports
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB Service 20 Info
 Admin : Up,  Oper : Up,  Stats : N,  Mtu : 9194, VlanXlation : N,
 ISID : 2524, BVlan : 4004, MCast-Mode : Headend, Tx/Rx : 0/0, RemoveIngTag: N,

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp SystemId:BVlan</th>
<th>Intf</th>
<th>Sdp SystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/23:0</td>
<td>Down</td>
<td>Down</td>
<td>N</td>
<td>Y:x</td>
<td>1/23</td>
<td>-</td>
</tr>
<tr>
<td>sap:1/23:9.10</td>
<td>Down</td>
<td>Down</td>
<td>N</td>
<td>Y:x</td>
<td>1/23</td>
<td>-</td>
</tr>
</tbody>
</table>
```

Total Ports: 2

```
-> show service 1 ports
Legend: (*) dyn unicast object
VxLAN Service 1 Info
 Admin : Up,  Oper : Up,  Stats : Y,  VlanXlation : Y,
 VNID : 1000 (0.1.56), MCast-Mode : Tandem, RemoveIngTag: N

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp FarEnd/Group</th>
<th>Intf</th>
<th>Sdp Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/3:0</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>Y:x</td>
<td>1/20</td>
<td>-</td>
</tr>
<tr>
<td>sap:1/3:10</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>Y:x</td>
<td>1/20</td>
<td>-</td>
</tr>
<tr>
<td>sdp:32770:1*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.2</td>
<td>1/1/1</td>
<td>PIM Group 224.2.1.1</td>
</tr>
<tr>
<td>sdp:32771:1*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.3</td>
<td>1/1/2</td>
<td>PIM Group 224.2.1.1</td>
</tr>
<tr>
<td>sdp:32772:1*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.4</td>
<td>1/1/1</td>
<td>PIM Group 224.2.1.1</td>
</tr>
</tbody>
</table>
```

Total Ports: 5

-> show service vnid 1000 ports
Legend: (*) dyn unicast object
VxLAN Service 1 Info
   Admin : Up,   Oper : Up,   Stats : Y,   VlanXlation : Y,
   VNID : 1000 (0.1.56),   MCast-Mode : Tandem,   RemoveIngTag: N

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp FarEnd/Group</th>
<th>Intf</th>
<th>Sdp Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/3:0</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>Y:x</td>
<td>1/20</td>
<td>-</td>
</tr>
<tr>
<td>sap:1/3:10</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>Y:x</td>
<td>1/20</td>
<td>-</td>
</tr>
<tr>
<td>sdp:10:1</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>224.2.1.1</td>
<td>-</td>
<td>PIM Group 224.2.1.1</td>
</tr>
<tr>
<td>sdp:32770:1*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.2</td>
<td>1/1/1</td>
<td>PIM Group 224.2.1.1</td>
</tr>
<tr>
<td>sdp:32771:1*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.3</td>
<td>1/1/2</td>
<td>PIM Group 224.2.1.1</td>
</tr>
<tr>
<td>sdp:32772:1*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.4</td>
<td>1/1/1</td>
<td>PIM Group 224.2.1.1</td>
</tr>
</tbody>
</table>

Total Ports: 5

-> show service 32770 ports
Legend: * denotes a dynamic object
L2GRE Service 32770 (Dynamic Service vpnid=123 for UNP)
   Admin : Up,   Oper : Up,   Stats : Y,   VlanXlation : Y,
   VPNID : 100,   RemoveIngTag: N

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp FarEnd/Group</th>
<th>Intf</th>
<th>Sdp Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/3:10</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>Y:x</td>
<td>1/1/3</td>
<td>L2GRE Loopback</td>
</tr>
<tr>
<td>sdp:33001:32770*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.2</td>
<td>1/1/1</td>
<td>L2GRE VPNID 100</td>
</tr>
</tbody>
</table>

Total Ports: 2

-> show service vpnid 100 ports
Legend: * denotes a dynamic object
L2GRE Service 32770 (Dynamic Service vpnid=123 for UNP)
   Admin : Up,   Oper : Up,   Stats : Y,   VlanXlation : Y,
   VPNID : 100,   RemoveIngTag: N

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp FarEnd/Group</th>
<th>Intf</th>
<th>Sdp Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/3:10</td>
<td>Up</td>
<td>Up</td>
<td>N</td>
<td>Y:x</td>
<td>1/1/3</td>
<td>L2GRE Loopback</td>
</tr>
<tr>
<td>sdp:33001:32770*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.2</td>
<td>1/1/1</td>
<td>L2GRE VPNID 100</td>
</tr>
<tr>
<td>sdp:33002:32771*</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td>10.10.10.3</td>
<td>1/1/2</td>
<td>L2GRE VPNID 100</td>
</tr>
</tbody>
</table>

Total Ports: 3

**output definitions**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>The virtual ports (SAPs or SDPs) associated with the service.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the virtual port (Up or Down).</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the virtual port (Up or Down).</td>
</tr>
<tr>
<td>Stats</td>
<td>Whether or not statistics collection is enabled for the virtual port.</td>
</tr>
<tr>
<td>Sap Trusted:Priority</td>
<td>Whether or not the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.</td>
</tr>
</tbody>
</table>
### Service Manager Commands

**show service ports**

#### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sdp SystemId : BVlan</td>
<td>The system ID (base MAC) and associated BVLAN for a Service Distribution Point (SDP) virtual port associated with the SPB service.</td>
</tr>
</tbody>
</table>
| Sdp FarEnd/Group    | - **VXLAN service**: The Loopback0 IP address or the multicast group IP address for the far-end VXLAN node associated with the service.  
                        - **L2 GRE service**: The Loopback0 IP address of the far-end Guest Tunnel access switch that is associated with the service. |
| Intf                | The bridge interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service. |
| Sap Description     | The description for the SAP that is associated with the service. |
| Sdp Systemname      | The system name for the SDP bridge that is associated with the SPB service. |
| Sdp Intf Name       | The description for the SDP interface that is associated with the VXLAN or L2 GRE service. |

#### Release History

- Release 7.3.1; command was introduced.
- Release 7.3.4; **vnid** parameter added for VXLAN services.
- Release 8.4.1.R02; **vpnid** parameter added for L2 GRE tunnel services.
- Release 8.7R2; “PW-Enb” field added only to the display output for SPB pseudo-wire services.

#### Related Commands

- **show service**  
  Displays the service configuration for the bridge.
- **show service spb sap**  
  Displays the service access point (SAP) configuration for a specific SAP associated with the specified SPB service.

#### MIB Objects

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
show service spb sap

Displays the configuration information for the specified Service Access Point (SAP) ID associated with the specified service. A SAP ID is comprised of a customer-facing port (referred to as an access port) and an encapsulation value that is used to identify the type of customer traffic to map to the associated service.

show service spb service_id sap {port chassis/slot/port | linkagg agg_num} [:0 | :all | :qtag] [:outer_qtag.inner_qtag]

Syntax Definitions

- service_id: An existing service ID number.
- chassis/slot/port: The slot and port number of the Service Access Port.
- agg_num: The link aggregate ID number (0–31) of a service access link aggregate.
- :0: Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
- :all: Specifies a wildcard SAP. All tagged traffic that is not classified into another SAP is mapped to the wildcard SAP.
- :qtag: Specifies a VLAN ID tag for traffic ingressing on the access port. Only traffic with this tag is mapped to this SAP.
- :outer_qtag.inner_qtag: Specifies an outer VLAN ID tag and an inner VLAN tag for traffic ingressing on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- A SAP is a type of virtual port that is associated with the specified service.
- A SAP determines which traffic (untagged, single-tagged, or double-tagged) is mapped to the service associated with this SAP.
Examples

-> show service spb 525 sap port 1/11:2524
SAP Detailed Info
   SAP Id           : 1/11:2524,            Description      : ,
   Admin Status     : Up,                   Oper Status      : Up,
   Stats Status     : No,                   Vlan Translation : No,
   Service Type     : SPB,                  Allocation Type  : Static,
   Trusted          : Yes,                  Priority         : 0,
   Ingress Pkts     : 0,                    Ingress Bytes    : 0,
   Egress Pkts      : 0,                    Egress Bytes     : 0,

-> show service spb 200 sap port 2/10:500
SAP Detailed Info
   SAP Id           : 2/10:500,             Description      : ,
   Admin Status     : Up,                   Oper Status      : Up,
   Stats Status     : No,                   Vlan Translation : No,
   Service Type     : VXLAN,                Allocation Type  : Static,
   Trusted          : Yes,                  Priority         : 0,
   Ingress Pkts     : 0,                    Ingress Bytes    : 0,
   Egress Pkts      : 0,                    Egress Bytes     : 0,

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Id</td>
<td>The access port and encapsulation associated with the service.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional description configured for the SAP. By default, the description is blank.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The administrative state of the SAP (Up or Down).</td>
</tr>
<tr>
<td>Oper Status</td>
<td>The operational state of the SAP (Up or Down).</td>
</tr>
<tr>
<td>Stats Status</td>
<td>Whether statistics collection is enabled for the SAP (Yes or No).</td>
</tr>
<tr>
<td>Vlan Translation</td>
<td>Whether VLAN translation is enabled for the SAP (Yes or No).</td>
</tr>
<tr>
<td>Service Type</td>
<td>The type of service associated with this SAP (SPB or VXLAN).</td>
</tr>
<tr>
<td>Allocation Type</td>
<td>Whether the service was manually or dynamically created (Static or Dynamic).</td>
</tr>
<tr>
<td>Trusted</td>
<td>Whether the SAP is trusted (Yes or No).</td>
</tr>
<tr>
<td>Priority</td>
<td>The 802.1p priority assigned to traffic mapped to this SAP. Applied only when the SAP is not trusted and a priority is specified.</td>
</tr>
<tr>
<td>Ingress Pkts</td>
<td>The number of packets that have ingressed on this SAP.</td>
</tr>
<tr>
<td>Ingress Bytes</td>
<td>The number of bytes that have ingressed on this SAP.</td>
</tr>
<tr>
<td>Egress Pkts</td>
<td>The number of packets that have egressed on this SAP.</td>
</tr>
<tr>
<td>Egress Bytes</td>
<td>The number of bytes that have egressed on this SAP.</td>
</tr>
<tr>
<td>Mgmt Change</td>
<td>The date and time of the last configuration change for this SAP.</td>
</tr>
<tr>
<td>Status Change</td>
<td>The date and time of the last operational status change for this SAP.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command was introduced.
**Related Commands**

- **show service**
  Displays the service configuration for the bridge.

- **show service ports**
  Displays the virtual ports (SAP and SDPs) associated with the specified SPB or VXLAN service.

**MIB Objects**

- **alaSapBaseInfoTable**
  - **alaSapSvcId**
  - **alaSapPortId**
  - **alaSapEncapValue**
  - **alaSapDescription**
  - **alaSapAdminStatus**
  - **alaSapOperStatus**
  - **alaSapStatsAdminStatus**
  - **alaSapType**
  - **alaSapAllocationType**
  - **alaSapTrusted**
  - **alaSapPriority**
  - **alaSapIngressPacketCount**
  - **alaSapIngressByteCount**
  - **alaSapEgressPacketCount**
  - **alaSapEgressByteCount**
  - **alaSapLastMgmtChange**
  - **alaSapLastStatusChange**

- **alaServiceMgrPortTable**
  - **alaServiceMgrPortID**
  - **alaServiceMgrPortVlanXlation**
**show service sdp**

Displays the Service Distribution Point (SDP) configuration for the bridge. An SDP is a logical service entity that tunnels traffic from one switch to another switch in the network.

```
show service sdp [sdp_id]
```

---

**Syntax Definitions**

*sdp_id*  
An existing SDP ID number.

**Defaults**

By default, all SDPs are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *sdp_id* parameter to display information about a specific SDP.
- Manual configuration of SDPs and SDP bindings is *not* required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDPs are not saved to the switch configuration file.
- Manual configuration of SDPs and SDP bindings is required for VXLAN services.
- The status of automatic discovery for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the *show service sdp l2gre* command for more information.
- Displaying the SDP configuration for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

**Examples**

```
-> show service sdp
Legend: * denotes a dynamic object
All SDP Info
          FarEnd/Group Ip Addr
SdpId  FarEnd SysId:Bvlan  Adm  Oper  SvcType
-----------------+---------------------+----+----+--------
10            224.2.1.1  Up  Up  VxLAN
```
20 10.10.10.2  Up  Up  VxLAN
30 10.10.10.3  Up  Up  VxLAN
40 10.10.10.4  Up  Up  L2GRE
32768* 00e0.b1e4.f5eb:4000  Up  Up  SPB
32769* 00e0.b1e7.067f:4000  Up  Up  SPB
33001* 10.10.10.2  Up  Up  L2GRE

Total SDPs: 5

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SdpId</td>
<td>A unique SDP identification number, dynamically generated by ISIS-SPB or manually configured for VXLAN services or L2 GRE tunnel services.</td>
</tr>
<tr>
<td>FarEnd/Group Addr</td>
<td>The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses.</td>
</tr>
<tr>
<td>FarEnd SysId:BVlan</td>
<td>The System ID (bridge MAC address) and associated BVLAN of the far-end SPB node of the tunnel defined by this SDP.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the SDP (Up or Down).</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the SDP (Up or Down).</td>
</tr>
<tr>
<td>Svc Type</td>
<td>The type of service traffic that this SDP will tunnel (SPB, VxLAN, or L2GRE).</td>
</tr>
</tbody>
</table>

-> show service sdp 10
VxLAN SDP 10 Info
SDP-Id : 10,  Description : 224.2.1.1 Group,
Service Type : VxLAN,  FarEnd/Group : 224.2.1.1,
Admin Status : Up,  Oper Status : Up,
TTL : 64 (default),
Allocation Type : Static,  SDP Bind Count : 3,

-> show service sdp 33001
L2GRE SDP 33001 Info
SDP-Id : 33001,  Description : L2GRE VPNID 100,
Service Type : L2GRE,  FarEnd/Group : 10.10.10.2,
Admin Status : Up,  Oper Status : Up,
TTL : 64 (default),
Allocation Type : Dynamic,  SDP Bind Count : 1,

SDP-Id: A unique SDP identification number manually configured for VXLAN services.
Description: An optional ASCII text description for this SDP.
Service Type: The type of service traffic that this SDP will tunnel (SPB, VxLAN, or L2GRE).
FarEnd/Group: The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses.
Admin Status: The administrative state of the SDP (Up or Down).
Oper Status: The operational state of the SDP (Up or Down).
Service Manager Commands

**show service sdp**

<table>
<thead>
<tr>
<th><strong>TTL</strong></th>
<th>The time-to-live (TTL) value for this SDP.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allocation Type</strong></td>
<td>Whether the SDP was statically or dynamically created. An SDP for an SPB service is generated dynamically; an SDP for a VXLAN or L2GRE tunnel service is generated statically or dynamically through the UNP feature.</td>
</tr>
<tr>
<td><strong>SDP Bind Count</strong></td>
<td>The number of services bound to this SDP.</td>
</tr>
<tr>
<td><strong>Mgmt Change</strong></td>
<td>The date and time of the last manual change to this SDP.</td>
</tr>
<tr>
<td><strong>Status Change</strong></td>
<td>The date and time of the last status change to this SDP.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN fields added.
Release 8.4.1.R02; L2 GRE fields added.

**Related Commands**

- `show service sdp spb` Displays SDP information specific to SPB services.
- `show service sdp vxlan` Displays SDP information specific to VXLAN services.
- `show service sdp l2gre` Displays SDP information specific to L2 GRE tunnel services.
- `show service` Displays the service configuration for the bridge.
- `show service bind-sdp` Displays the Mesh SDP configuration for the bridge.

**MIB Objects**

- `alaSdpInfoTable`<br>  
  - `alaSdpId`  
  - `alaSdpSvcType`  
  - `alaSdpDelivery`  
  - `alaSdpFarEndIpAddress`  
  - `alaSdpDescription`  
  - `alaSdpAdminStatus`  
  - `alaSdpOperStatus`  
  - `alaSdpLastMgmtChange`  
  - `alaSdpLastStatusChange`  
  - `alaSdpNetworkPort`  
  - `alaSdpBVlan`  
  - `alaSdpSystemId`  
  - `alaSdpSystemName`  
  - `alaSdpSpSourceId`  
  - `alaSdpAllocationType`  
  - `alaSdpDynamicType`  
  - `alaSdpBindCount`  
  - `alaSdpIsid`  
  - `alaSdpMcastPortList`  
  - `alaSdpCreationOrigin`  
  - `alaSdpAdminTTL`
**show service sdp spb**

Displays the Service Distribution Point (SDP) configuration for SPB services.

```plaintext
show service sdp spb [sysid mac_address | bvlan bvlan_id]
```

### Syntax Definitions

- **mac_address**
  
  The System ID (BMAC) of the far-end SPB node of the service tunnel defined by this SDP.

- **bvlan_id**
  
  The VLAN ID number of an existing SPB BVLAN.

### Defaults

By default, all SDPs are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **sysid** and **bvlan** parameters to display additional information about SPB SDPs.
- Manual configuration of SDPs and SDP bindings is *not* required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDPs are not saved to the switch configuration file.

### Examples

```plaintext
-> show service sdp spb
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object

SPB SDP Info

<table>
<thead>
<tr>
<th>SdpId</th>
<th>SysId:BVlan/GroupMac</th>
<th>SourceId</th>
<th>Oper</th>
<th>Intf/Isid Count</th>
<th>SystemName/PortList</th>
</tr>
</thead>
<tbody>
<tr>
<td>32768</td>
<td>00e0.b1e4.067f:4001</td>
<td>0x70bd3</td>
<td>Up</td>
<td>1/3</td>
<td>0</td>
</tr>
<tr>
<td>32769</td>
<td>00e0.b1e7.067f:4002</td>
<td>0x70bd3</td>
<td>Up</td>
<td>1/2</td>
<td>0</td>
</tr>
</tbody>
</table>

Total SDPs: 2
```
-> show service sdp spb sysid 00.e0.b1.e4.06.7f
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB SDP Info
<table>
<thead>
<tr>
<th>FarEnd</th>
<th>Bind FarEnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>SdpId</td>
<td>SysId:BVlan/GroupMac</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>32768*</td>
<td>00e0.b1e4.067f:4001</td>
</tr>
</tbody>
</table>
Total SDPs: 1

-> show service sdp spb bvlan 4002
Legend: (*) dyn unicast object (+) remote mcast object (#) local mcast object
SPB SDP Info
<table>
<thead>
<tr>
<th>FarEnd</th>
<th>Bind FarEnd</th>
</tr>
</thead>
<tbody>
<tr>
<td>SdpId</td>
<td>SysId:BVlan/GroupMac</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>32769*</td>
<td>00e0.b1e7.067f:4002</td>
</tr>
</tbody>
</table>
Total SDPs: 1

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SdpId</td>
<td>The unique SDP identification number that is dynamically generated by ISIS-SPB.</td>
</tr>
<tr>
<td>FarEnd SysId:BVlan/GroupMac</td>
<td>The System ID (BMAC) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.</td>
</tr>
<tr>
<td>SourceId</td>
<td>The shortest path (SP) source ID of the bridge.</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the SDP (Up or Down).</td>
</tr>
<tr>
<td>Intf/Isid</td>
<td>The SPB interface (network port) on which ISIS-SPB discovered the neighbor BMAC and BVLAN.</td>
</tr>
<tr>
<td>Bind Count</td>
<td>The number of services bound to this SDP.</td>
</tr>
<tr>
<td>FarEnd SystemName/PortList</td>
<td>The system name and port list of the far-end SPB node.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; **sysid** and **bvlan** parameters added.

**Related Commands**

- `show service sdp` Displays the SDP configuration for the switch.
- `show service sdp vxlan` Displays SDP information specific to VXLAN services.
- `show service sdp l2gre` Displays SDP information specific to L2 GRE tunnel services.
- `show service` Displays the service configuration for the bridge.
- `show service bind-sdp` Displays the Mesh SDP configuration for the bridge.
**MIB Objects**

alaSdpInfoTable
  alaSdpId
  alaSdpSvcType
  alaSdpDelivery
  alaSdpFarEndIpAddress
  alaSdpDescription
  alaSdpAdminStatus
  alaSdpOperStatus
  alaSdpLastMgmtChange
  alaSdpLastStatusChange
  alaSdpNetworkPort
  alaSdpBVlan
  alaSdpSystemId
  alaSdpSystemName
  alaSdpSpSourceId
  alaSdpAllocationType
  alaSdpDynamicType
  alaSdpBindCount
  alaSdpIsid
  alaSdpMcastPortList
  alaSdpCreationOrigin
  alaSdpAdminTTL
**show service sdp vxlan**

Displays the Service Distribution Point (SDP) configuration for Virtual eXtensible LAN (VXLAN) services.

**show service sdp vxlan [far-end ip_address | multicast-group mc_group_address]**

---

**Syntax Definitions**

- **ip_address**
  
  The IP address of the Loopback0 interface for the far-end VXLAN Tunnel End Point (VTEP) node. The Loopback0 address is required on every VTEP node.

- **mc_group_address**
  
  The multicast IP address of the group to which the service will join. This parameter is not supported on an OmniSwitch 6900-V72/C32.

---

**Defaults**

By default, all SDPs are displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **far-end** and **multicast-group** parameters to display only VXLAN SDPs associated with a specific far-end IP address or a specific multicast group IP address.

- Manual configuration of SDPs and SDP bindings for VXLAN services is required.

---

**Examples**

```plaintext
-> show service sdp vxlan
Legend: (*) dyn unicast object
VxLAN SDP Info

<table>
<thead>
<tr>
<th>SdpId</th>
<th>FarEnd/Group Addr</th>
<th>Adm</th>
<th>Oper Intf</th>
<th>Bind Count</th>
<th>TTL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>224.2.1.1</td>
<td>Up</td>
<td>Up</td>
<td>3</td>
<td>64</td>
<td>224.2.1.1 Group</td>
</tr>
<tr>
<td>20</td>
<td>10.10.10.2</td>
<td>Up</td>
<td>Up 1/1/1</td>
<td>2</td>
<td>64</td>
<td>To NodeB</td>
</tr>
<tr>
<td>30</td>
<td>10.10.10.3</td>
<td>Up</td>
<td>Up 1/1/2</td>
<td>1</td>
<td>64</td>
<td>To NodeC</td>
</tr>
</tbody>
</table>
```
Service Manager Commands

$show service sdp vxlan multicast-group 224.2.1.1$

Legend: (*) dyn unicast object

VxLAN SDP Info

<table>
<thead>
<tr>
<th>SdpId</th>
<th>FarEnd/Group Addr</th>
<th>Adm</th>
<th>Oper</th>
<th>Intf</th>
<th>Bind</th>
<th>Count</th>
<th>TTL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>224.2.1.1</td>
<td>Up</td>
<td>Up</td>
<td>-</td>
<td>3</td>
<td>64</td>
<td></td>
<td>224.2.1.1 Group</td>
</tr>
</tbody>
</table>

Total SDPs: 1

$show service sdp vxlan far-end 10.10.10.2$

Legend: (*) dyn unicast object

VxLAN SDP Info

<table>
<thead>
<tr>
<th>SdpId</th>
<th>FarEnd/Group Addr</th>
<th>Adm</th>
<th>Oper</th>
<th>Intf</th>
<th>Bind</th>
<th>Count</th>
<th>TTL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>10.10.10.2</td>
<td>Up</td>
<td>Up</td>
<td>1/1/1</td>
<td>2</td>
<td>64</td>
<td></td>
<td>To NodeB</td>
</tr>
</tbody>
</table>

Total SDPs: 1

**SdpId**
A unique SDP identification number manually configured for VXLAN services.

**FarEnd/Group Addr**
The IP address (Loopback0) or multicast group IP address associated with the far-end VXLAN node of this SDP.

**Adm**
The administrative state of the SDP (**Up** or **Down**).

**Oper**
The operational state of the SDP (**Up** or **Down**).

**Intf**
The VXLAN interface on which the VXLAN node was discovered for a unicast SDP (this field is blank for a multicast SDP).

**Bind Count**
The number of services bound to this SDP.

**ttl**
The time-to-live (TTL) value for this SDP.

**Description**
An optional ASCII text description for this SDP.

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- **service sdp vxlan**
  Configures an SDP for a VXLAN service.

- **show service sdp**
  Displays the SDP configuration for the switch.

- **show service sdp spb**
  Displays SDP information specific to SPB services.

- **show service sdp l2gre**
  Displays SDP information specific to L2 GRE tunnel services.

- **show service**
  Displays the service configuration for the bridge.

- **show service bind-sdp**
  Displays the Mesh SDP configuration for the bridge.
### MIB Objects

<table>
<thead>
<tr>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaSdpInfoTable</td>
</tr>
<tr>
<td>alaSdpId</td>
</tr>
<tr>
<td>alaSdpSvctype</td>
</tr>
<tr>
<td>alaSdpDelivery</td>
</tr>
<tr>
<td>alaSdpFarEndIpAddress</td>
</tr>
<tr>
<td>alaSdpDescription</td>
</tr>
<tr>
<td>alaSdpAdminStatus</td>
</tr>
<tr>
<td>alaSdpOperStatus</td>
</tr>
<tr>
<td>alaSdpLastMgmtChange</td>
</tr>
<tr>
<td>alaSdpLastStatusChange</td>
</tr>
<tr>
<td>alaSdpNetworkPort</td>
</tr>
<tr>
<td>alaSdpBVlan</td>
</tr>
<tr>
<td>alaSdpSystemId</td>
</tr>
<tr>
<td>alaSdpSystemName</td>
</tr>
<tr>
<td>alaSdpSpSourceId</td>
</tr>
<tr>
<td>alaSdpAllocationType</td>
</tr>
<tr>
<td>alaSdpDynamicType</td>
</tr>
<tr>
<td>alaSdpBindCount</td>
</tr>
<tr>
<td>alaSdpIsid</td>
</tr>
<tr>
<td>alaSdpMcastPortList</td>
</tr>
<tr>
<td>alaSdpCreationOrigin</td>
</tr>
<tr>
<td>alaSdpAdminTTL</td>
</tr>
</tbody>
</table>
**show service sdp l2gre**

Displays the Service Distribution Point (SDP) configuration for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services.

**show service sdp l2gre [far-end ip_address]**

---

**Syntax Definitions**

*ip_address*  
The IP address of the Loopback0 interface for the far-end L2GRE tunnel endpoint. The Loopback0 address is required on every VTEP node.

---

**Defaults**

By default, all SDPs are displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **far-end** parameter to display only L2 GRE SDPs associated with a specific far-end IP address; multicast group IP addresses are not supported.

- The status of automatic SDP discovery for L2 GRE tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the **service l2gre auto-discover** command for more information.
  - If L2 GRE automatic discovery is enabled (the default), then SDPs are automatically created and bound to L2 GRE services.
  - If L2 GRE automatic discovery is disabled, then manual configuration of SDPs and SDP bindings is required for L2 GRE services.

- This command is supported on an OmniSwitch 6560 to display dynamically configured L2 GRE service objects, such as SDPs.

---

**Examples**

```bash
-> show service sdp l2gre
Legend: (*) dyn unicast object
L2GRE SDP Info

<table>
<thead>
<tr>
<th>SdpId</th>
<th>FarEnd Addr</th>
<th>Adm</th>
<th>Oper</th>
<th>Intf</th>
<th>Bind</th>
<th>Count</th>
<th>TTL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33001*</td>
<td>10.10.10.2</td>
<td>Up</td>
<td>Up</td>
<td>1/1/1</td>
<td>1</td>
<td>64</td>
<td>64</td>
<td>L2GRE VPNID 100</td>
</tr>
<tr>
<td>33002*</td>
<td>10.10.10.3</td>
<td>Up</td>
<td>Up</td>
<td>1/1/2</td>
<td>1</td>
<td>64</td>
<td>64</td>
<td>L2GRE VPNID 100</td>
</tr>
</tbody>
</table>
```

---
-> show service sdp l2gre far-end 10.10.10.2

Legend: (*) dyn unicast object

<table>
<thead>
<tr>
<th>SdpId</th>
<th>FarEnd Addr</th>
<th>Adm</th>
<th>Oper</th>
<th>Intf</th>
<th>Count</th>
<th>TTL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33001*</td>
<td>10.10.10.2</td>
<td>Up</td>
<td>Up</td>
<td>1/1/1</td>
<td>1</td>
<td>64</td>
<td>L2GRE VPNID 100</td>
</tr>
</tbody>
</table>

**SdpId**
A unique SDP identification number manually configured for L2 GRE services.

**FarEnd Addr**
The IP address (Loopback0 interface) associated with the far-end L2 GRE tunnel endpoint of this SDP.

**Adm**
The administrative state of the SDP (**Up** or **Down**).

**Oper**
The operational state of the SDP (**Up** or **Down**).

**Intf**
The interface on which the L2 GRE tunnel endpoint was discovered for a unicast SDP.

**Bind Count**
The number of services bound to this SDP.

**ttl**
The time-to-live (TTL) value for this SDP.

**Description**
An optional ASCII text description for this SDP.

**Release History**
Release 8.4.1.R02; command was introduced.

**Related Commands**
- `service sdp l2gre` Configures an SDP for an L2 GRE tunnel service.
- `show service sdp` Displays the SDP configuration for the switch.
- `show service sdp spb` Displays SDP information specific to SPB services.
- `show service sdp vxlan` Displays SDP information specific to VXLAN services.
- `show service` Displays the service configuration for the bridge.
- `show service bind-sdp` Displays the Mesh SDP configuration for the bridge.
MIB Objects

alaSdpInfoTable
  alaSdpId
  alaSdpSvcType
  alaSdpDelivery
  alaSdpFarEndIpAddress
  alaSdpDescription
  alaSdpAdminStatus
  alaSdpOperStatus
  alaSdpLastMgmtChange
  alaSdpLastStatusChange
  alaSdpNetworkPort
  alaSdpBVlan
  alaSdpSystemId
  alaSdpSystemName
  alaSdpSpSourceId
  alaSdpAllocationType
  alaSdpDynamicType
  alaSdpBindCount
  alaSdpIsid
  alaSdpMcastPortList
  alaSdpCreationOrigin
  alaSdpAdminTTL
show service bind-sdp

Displays the Service Distribution Point (SDP) binding configuration for the switch.

`show service bind-sdp [sdp_id[:service_id]]`

**Syntax Definitions**

- `sdp_id[:service_id]` Displays SDP bindings with the specified SDP ID and/or service ID number.

**Defaults**

By default, all SDP bindings are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Manual configuration of SDPs and SDP bindings is **not** required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.

- Dynamic SDP bindings are not saved to the switch configuration file.

- Manual configuration of SDPs and SDP bindings is required for VXLAN services.

- The status of automatic SDP discovery for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the `show service bind-sdp l2gre` command for more information.

- This command is also supported on an OmniSwitch 6560 to display dynamically configured L2 GRE service objects, such as SDP bindings.

- The `show service bind-sdp` command is the preferred command to use for displaying the SDP binding configuration, instead of the `show service mesh-sdp` command.

- Displaying the SDP binding configuration for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
Examples

-> show service bind-sdp
Legend: * denotes a dynamic object
All Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>FarEnd/Group Addr</th>
<th>FarEnd SysId:BVlan</th>
<th>Oper</th>
<th>SvcType</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:1</td>
<td>1.1.1.6</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>1</td>
<td>20:1</td>
<td>1.1.1.2</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>1</td>
<td>30:1</td>
<td>1.1.1.3</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>1</td>
<td>100:1</td>
<td>224.1.1.1.100</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>10:2</td>
<td>1.1.1.6</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>20:2</td>
<td>1.1.1.2</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>30:2</td>
<td>1.1.1.3</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>200:2</td>
<td>224.1.1.1.200</td>
<td></td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>3</td>
<td>220:3</td>
<td>11.2.2.1</td>
<td></td>
<td>Up</td>
<td>L2GRE</td>
</tr>
<tr>
<td>100</td>
<td>32768:100*</td>
<td>00e0.ble4.f5eb:4000</td>
<td></td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>100</td>
<td>32769:100*</td>
<td>e8e7.3211.cdb9:4000</td>
<td></td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>200</td>
<td>32769:200*</td>
<td>e8e7.3211.cdb9:4000</td>
<td></td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>300</td>
<td>32769:300*</td>
<td>e8e7.3211.cdb9:4000</td>
<td></td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>32771*</td>
<td>33002:32771*</td>
<td>10.10.10.3</td>
<td></td>
<td>Down</td>
<td>L2GRE</td>
</tr>
</tbody>
</table>

Total Bind-SDPs: 14

output definitions

SvcId
The ID number of the service that is bound to the SDP.

Bind-SDP
The unique SDP identification number that is bound to the service number.

FarEnd/Group Addr
The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses.

FarEnd SysId:BVlan
The System ID (bridge MAC address) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.

Oper
The operational state of the SDP binding (Up or Down).

Svc Type
The type of service bound to the SDP (SPB, VXLAN, or L2GRE).

-> show service bind-sdp 10
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>Vnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper Intf</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:1</td>
<td>100</td>
<td>1.1.1.6</td>
<td>Up</td>
<td>Intf-101</td>
</tr>
<tr>
<td>2</td>
<td>10:2</td>
<td>200</td>
<td>1.1.1.6</td>
<td>Up</td>
<td>Intf-101</td>
</tr>
</tbody>
</table>

Total Bind-SDPs: 2

-> show service bind-sdp 30:2
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>Vnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper Intf</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>30:2</td>
<td>200</td>
<td>1.1.1.3</td>
<td>Up</td>
<td>Intf-101</td>
</tr>
</tbody>
</table>

Total Bind-SDPs: 1
Service Manager Commands

-> show service bind-sdp 220
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>Vpnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>220:3</td>
<td>300</td>
<td>11.2.2.1</td>
<td>Down</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Total Bind-SDPs: 1

-> show service bind-sdp 33002:32771
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>Vpnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>32771</td>
<td>33002:32771*</td>
<td>400</td>
<td>10.10.10.3</td>
<td>Down</td>
<td>-</td>
</tr>
</tbody>
</table>

Total Bind-SDPs: 1

Output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SvcId</td>
<td>The ID number of the service that is bound to the SDP.</td>
</tr>
<tr>
<td>Bind-SDP</td>
<td>The unique SDP identification number that is bound to the service number. For example, 220:3 represents SDP 220 bound to service 3.</td>
</tr>
<tr>
<td>Vnid or Vpnid</td>
<td>A 24-bit numerical value that identifies a VXLAN segment ID (Vnid) or an L2 GRE tunnel segment ID (Vpnid).</td>
</tr>
<tr>
<td>FarEnd/Group Addr</td>
<td>The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses.</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the SDP binding (Up or Down).</td>
</tr>
<tr>
<td>Intf</td>
<td>The VXLAN or L2 GRE interface on which the SDP binding was configured.</td>
</tr>
<tr>
<td>Intf Name</td>
<td>The name assigned to the VXLAN or L2 GRE interface.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN fields added.
Release 8.4.1.R02; L2 GRE fields added.

Related Commands

show service bind-sdp spb  | Displays SDP binding information for SPB services.        |
show service bind-sdp vxlan | Displays SDP binding information for VXLAN services.      |
show service bind-sdp l2gre | Displays SDP binding information for L2 GRE tunnel services. |
show service l2gre           | Displays the service configuration for the bridge.         |
show service sdp             | Displays the SDP configuration for the bridge.             |
MIB Objects

alaSdpBindTable
  alaSdpBindId
  alaSdpBindOperStatus
  alaSdpBindNetworkPort
  alaSdpBindVirtualPort
  alaSdpBindIsid
  alaSdpBindBVlan
  alaSdpBindSystemId
  alaSdpBindSystemName
  alaSdpBindAllocationType
  alaSdpBindCreationOrigin
  alaSdpBindFarEndIpAddress
  alaSdpBindVnid
show service bind-sdp spb

Displays the Service Distribution Point (SDP) binding configuration for Shortest Path Bridging (SPB) services.

show service bind-sdp [spb | isid instance_id]

Syntax Definitions

spb
Displays SPB SDP bindings.

instance_id
Displays SPB SDP bindings associated with the specified service instance identifier (I-SID) number. The valid range is 256–16777214.

Defaults

By default, all SDP bindings are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the spb parameter to display information for all SPB bindings.
- Use the isid parameter to display information for a specific SPB service instance.
- Manual configuration of SDPs and SDP bindings is not required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDP bindings are not saved to the switch configuration file.

Examples

-> show service bind-sdp spb
Legend: * denotes a dynamic object
SPB Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>SdpId</th>
<th>Isid</th>
<th>FarEnd SysId:BVlan</th>
<th>Oper Intf</th>
<th>FarEnd SystemName</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>33687:1*</td>
<td>1000</td>
<td>e8e7.3233.1831:4001</td>
<td>Up 1/1</td>
<td>Bridge-4</td>
</tr>
<tr>
<td>1</td>
<td>37753:1*</td>
<td>1000</td>
<td>0000.bcb6.0001:4001</td>
<td>Up 1/1</td>
<td>Ix-SPB-6</td>
</tr>
<tr>
<td>1</td>
<td>38169:1*</td>
<td>1000</td>
<td>0000.bcb4.0001:4001</td>
<td>Up 1/1</td>
<td>Ix-SPB-4</td>
</tr>
<tr>
<td>1</td>
<td>38217:1*</td>
<td>1000</td>
<td>0000.beb4.0001:4001</td>
<td>Up 1/1</td>
<td>Ix-BEB-4.1.1</td>
</tr>
<tr>
<td>1</td>
<td>38218:1*</td>
<td>1000</td>
<td>0000.beb4.0002:4001</td>
<td>Up 1/1</td>
<td>Ix-BEB-4.1.2</td>
</tr>
<tr>
<td>1</td>
<td>38219:1*</td>
<td>1000</td>
<td>0000.beb4.0003:4001</td>
<td>Up 1/1</td>
<td>Ix-BEB-4.1.3</td>
</tr>
<tr>
<td>1</td>
<td>38220:1*</td>
<td>1000</td>
<td>0000.beb4.0004:4001</td>
<td>Up 1/1</td>
<td>Ix-BEB-4.2.1</td>
</tr>
</tbody>
</table>
show service bind-sdp spb

1  38221:1*  1000  0000.beb4.0005:4001  Up  1/1  Ix-BEB-4.2.2
1  38222:1*  1000  0000.beb4.0006:4001  Up  1/1  Ix-BEB-4.2.3
1  38223:1*  1000  0000.beb4.0007:4001  Up  1/1  Ix-BEB-4.3.1

Total Bind-SDPs: 10

output definitions

SvcId
The ID number of the SPB service that is bound to the SDP.

SdpId
The unique SDP identification number that is dynamically generated by ISIS-SPB and bound to the service number.

Iсид
The service instance identifier (I-SID) number for the SPB service.

FarEnd SysId:BVlan
The System ID (BMAC) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.

Oper
The operational state of the SDP binding (Up or Down).

Intf
The SPB interface (network port) on which ISIS-SPB discovered the neighbor BMAC and BVLAN.

FarEnd SystemName
The system name of the far-end SPB node.

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; isid parameter added.

Related Commands

show service bind-sdp
Displays the SDP binding configuration for the switch.

show service bind-sdp vxlan
Displays SDP binding information for VXLAN services.

show service bind-sdp l2gre
Displays SDP binding information for L2 GRE tunnel services.

show service
Displays the service configuration for the bridge.

show service sdp
Displays the SDP configuration for the bridge.

MIB Objects

alaSdpBindTable

alaSdpBindId
alaSdpBindOperStatus
alaSdpBindNetworkPort
alaSdpBindVirtualPort
alaSdpBindIsid
alaSdpBindBVlan
alaSdpBindSystemId
alaSdpBindSystemName
alaSdpBindAllocationType
alaSdpBindCreationOrigin
alaSdpBindFarEndIpAddress
alaSdpBindVnid
show service bind-sdp vxlan

Displays the Service Distribution Point (SDP) binding configuration for Virtual eXtensible LAN (VXLAN) services.

show service bind-sdp [vxlan | vnid vxlan_id]

**Syntax Definitions**

- **vxlan**: Displays VXLAN SDP bindings.
- **vxlan_id**: An existing VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).

**Defaults**

By default, all SDP bindings are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **vxlan** parameter to display information for all VXLAN bindings.
- Use the **vnid** parameter to display information for a specific VNID.
- Manual configuration of SDPs and SDP bindings for VXLAN services is required.

**Examples**

```
-> show service bind-sdp vxlan
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info
SvcId Bind-Sdp Vnid FarEnd/Group Addr Oper Intf Intf Name
---------+----------------+--------+-----------------+рубу -     Intf-101
       1 10:1   100  1.1.1.6        Up  -     Intf-101
       1 20:1   100  1.1.1.2        Up  -     Intf-110
       1 30:1   100  1.1.1.3        Up  -     Intf-101
       1 100:1  100  224.1.1.100    Up  -     Intf-101
       2 10:2   200  1.1.1.6        Up  -     Intf-101
       2 20:2   200  1.1.1.2        Up  -     Intf-110
       2 30:2   200  1.1.1.3        Up  -     Intf-101
       2 200:2  200  224.1.1.200    Up  -     Intf-101

Total Bind-SDPs: 8
```
-> show service bind-sdp vnid 200
Legend: * denotes a dynamic object
VxLAN Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>Vnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper</th>
<th>Intf</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>10:2</td>
<td>200</td>
<td>1.1.1.6</td>
<td>Up</td>
<td>-</td>
<td>Intf-101</td>
</tr>
<tr>
<td>2</td>
<td>20:2</td>
<td>200</td>
<td>1.1.1.2</td>
<td>Up</td>
<td>-</td>
<td>Intf-110</td>
</tr>
<tr>
<td>2</td>
<td>30:2</td>
<td>200</td>
<td>1.1.1.3</td>
<td>Up</td>
<td>-</td>
<td>Intf-101</td>
</tr>
<tr>
<td>2</td>
<td>200:2</td>
<td>200</td>
<td>224.1.1.200</td>
<td>Up</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

Total Bind-SDPs: 4

SvcId
The ID number of the service that is bound to the SDP.

Bind-SDP
The unique SDP identification number that is bound to the service number. For example, 200:2 represents SDP 200 bound to service 2.

Vnid
A 24-bit numerical value that identifies a VXLAN segment.

FarEnd/Group Addr
The IP address (Loopback0) or multicast group IP address associated with the far-end VXLAN node of the SDP.

Oper
The operational state of the SDP binding (Up or Down).

Intf
The VXLAN interface on which the SDP binding was configured.

Intf Name
The name assigned to the VXLAN interface.

Release History
Release 7.3.4; command was introduced.

Related Commands
- show service bind-sdp: Displays the SDP binding configuration for the switch.
- show service bind-sdp spb: Displays SDP binding information for SPB services.
- show service bind-sdp l2gre: Displays SDP binding information for L2 GRE tunnel services.
- show service: Displays the service configuration for the bridge.
- show service sdp: Displays the SDP configuration for the bridge.

MIB Objects
alaSdpBindTable
  alaSdpBindId
  alaSdpBindOperStatus
  alaSdpBindNetworkPort
  alaSdpBindVirtualPort
  alaSdpBindIsid
  alaSdpBindBVlan
  alaSdpBindSystemId
  alaSdpBindSystemName
  alaSdpBindAllocationType
  alaSdpBindCreationOrigin
  alaSdpBindFarEndIpAddress
  alaSdpBindVnoid
show service bind-sdp l2gre

Displays the Service Distribution Point (SDP) binding configuration for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services.

show service bind-sdp [l2gre | vpnid vpn_id]

Syntax Definitions

l2gre Displays L2 GRE SDP bindings.
vpnid An existing VPN ID for an L2 GRE tunnel segment.

Defaults

By default, all SDP bindings are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the l2gre parameter to display information for all L2 GRE bindings.
- Use the vpnid parameter to display information for a specific L2 GRE VPN segment.
- The status of automatic SDP discovery for L2 GRE tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the service l2gre auto-discover command for more information.
  - If L2 GRE automatic discovery is enabled (the default), then SDPs are automatically created and bound to L2 GRE services.
  - If L2 GRE automatic discovery is disabled, then manual configuration of SDPs and SDP bindings is required for L2 GRE services.
- This command is supported on an OmniSwitch 6560 to display dynamically configured L2 GRE service objects, such as SDP bindings.

Examples

-> show service bind-sdp l2gre
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info
<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>Vpnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper Intf</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>220:3</td>
<td>300</td>
<td>11.2.2.1</td>
<td>Down</td>
<td>-</td>
</tr>
<tr>
<td>32771</td>
<td>33002:32771*</td>
<td>400</td>
<td>10.10.10.3</td>
<td>Down</td>
<td>-</td>
</tr>
</tbody>
</table>
Service Manager Commands

show service bind-sdp l2gre

Total Bind-SDPs: 2
-> show service bind-sdp vpnid 300
Legend: * denotes a dynamic object
L2GRE Bind-SDP Info

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-Sdp</th>
<th>Vpnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper</th>
<th>Intf</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>220:3</td>
<td>300</td>
<td>11.2.2.1</td>
<td>Down</td>
<td>-</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Total Bind-SDPs: 1

<table>
<thead>
<tr>
<th>SvcId</th>
<th>Bind-SDP</th>
<th>Vpnid</th>
<th>FarEnd/Group Addr</th>
<th>Oper</th>
<th>Intf</th>
<th>Intf Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>220:3</td>
<td>300</td>
<td>11.2.2.1</td>
<td>Down</td>
<td>-</td>
<td>vlan1</td>
</tr>
</tbody>
</table>

Legend: * denotes a dynamic object

**Release History**

Release 8.4.1.R02; command was introduced.

**Related Commands**

- **show service bind-sdp**
  - Displays the SDP binding configuration for the switch.
- **show service bind-sdp vxlan**
  - Displays SDP binding information for VXLAN services.
- **show service bind-sdp spb**
  - Displays SDP binding information for SPB services.
- **show service**
  - Displays the service configuration for the bridge.
- **show service sdp**
  - Displays the SDP configuration for the bridge.

**MIB Objects**

alaSdpBindTable
  - alaSdpBindId
  - alaSdpBindOperStatus
  - alaSdpBindNetworkPort
  - alaSdpBindVirtualPort
  - alaSdpBindIsid
  - alaSdpBindBVlan
  - alaSdpBindSystemId
  - alaSdpBindSystemName
  - alaSdpBindAllocationType
  - alaSdpBindCreationOrigin
  - alaSdpBindFarEndIpAddress
  - alaSdpBindVnid
show service mesh-sdp

Displays the bindings between services and Service Distribution Points (SDPs).

show service mesh-sdp

Syntax Definitions

sdp_id[;service_id] Displays SDP bindings with the specified SDP ID and/or service ID number.

Defaults

By default, all SDP bindings are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Manual configuration of SDPs and SDP bindings is not required for SPB services. SDPs are automatically created and bound to ISIS-SPB services as needed throughout the Provider Backbone Bridge (PBB) network.
- Dynamic SDP bindings are not saved to the switch configuration file.
- Manual configuration of SDPs and SDP bindings is required for VXLAN services.
- The status of automatic SDP discovery for Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel services determines whether or not manual configuration of SDPs and SDP bindings is required on an L2 GRE tunnel aggregation switch. See the show service bind-sdp l2gre command for more information.
- This command is also supported on an OmniSwitch 6560 to display dynamically configured L2 GRE service objects, such as SDPs.
- Displaying the SDP binding configuration for VXLAN services is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

Examples

```
-> show service mesh-sdp
Legend: * denotes a dynamic object
All Mesh-SDP Info
<table>
<thead>
<tr>
<th>SvcId</th>
<th>SdpId</th>
<th>FarEnd/Group Addr</th>
<th>FarEnd SysId:BVlan</th>
<th>Oper SvcType</th>
</tr>
</thead>
</table>
```

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 10-122
<table>
<thead>
<tr>
<th>SvcId</th>
<th>SdpId</th>
<th>FarEnd/Group Addr</th>
<th>Oper</th>
<th>Svc Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10:1</td>
<td>1.1.1.6</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>1</td>
<td>20:1</td>
<td>1.1.1.2</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>1</td>
<td>30:1</td>
<td>1.1.1.3</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>1</td>
<td>100:1</td>
<td>224.1.1.100</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>10:2</td>
<td>1.1.1.6</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>20:2</td>
<td>1.1.1.2</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>30:2</td>
<td>1.1.1.3</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>2</td>
<td>200:2</td>
<td>224.1.1.200</td>
<td>Up</td>
<td>VxLAN</td>
</tr>
<tr>
<td>3</td>
<td>220:3</td>
<td>11.2.2.1</td>
<td>Up</td>
<td>L2GRE</td>
</tr>
<tr>
<td>100</td>
<td>32768:100*</td>
<td>00e0.b1e4.f5eb:4000</td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>100</td>
<td>32769:100*</td>
<td>e8e7.3211.cdb9:4000</td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>200</td>
<td>32769:200*</td>
<td>e8e7.3211.cdb9:4000</td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>300</td>
<td>32769:300*</td>
<td>e8e7.3211.cdb9:4000</td>
<td>Up</td>
<td>SPB</td>
</tr>
<tr>
<td>32771*</td>
<td>33002:32771*</td>
<td>10.10.10.3</td>
<td>Down</td>
<td>L2GRE</td>
</tr>
</tbody>
</table>

Total Mesh-SDPs: 14

**output definitions**

- **SvcId**: The ID number of the service that is bound to the SDP.
- **SdpId**: The unique SDP identification number that is bound to the service number.
- **FarEnd/Group Addr**: The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses.
- **FarEnd SysId:BVlan**: The System ID (bridge MAC address) and associated BVLAN of the far-end SPB node of the PBB tunnel defined by this SDP.
- **Oper**: The operational state of the SDP binding (Up or Down).
- **Svc Type**: The type of service bound to the SDP (SPB, VXLAN, or L2GRE).

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; VXLAN fields added.
Release 8.4.1.R02; L2 GRE fields added.

**Related Commands**

- **show service bind-sdp spb**: Displays SDP binding information for SPB services.
- **show service bind-sdp vxlan**: Displays SDP binding information for VXLAN services.
- **show service bind-sdp l2gre**: Displays SDP binding information for L2 GRE tunnel services.
- **show service**: Displays the service configuration for the bridge.
- **show service sdp**: Displays the SDP configuration for the bridge.
MIB Objects

alaSdpBindTable
   alaSdpBindId
   alaSdpBindOperStatus
   alaSdpBindNetworkPort
   alaSdpBindVirtualPort
   alaSdpBindIsid
   alaSdpBindBVlan
   alaSdpBindSystemId
   alaSdpBindSystemName
   alaSdpBindAllocationType
   alaSdpBindCreationOrigin
   alaSdpBindFarEndIpAddress
   alaSdpBindVnid
show service debug-info

Displays debug information for the virtual ports associated with the service.

```
show service {service_id | isid instance_id | vnid vxlan_id | vpnid vpn_id} debug-info
```

**Syntax Definitions**

- **service_id**: An existing service ID number.
- **instance_id**: Displays debug information for the SPB service associated with the specified service instance identifier (I-SID) number. The valid range is 256–16777214.
- **vxlan_id**: Displays debug information for the VXLAN service associated with the specified VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).
- **vpnid**: Displays debug information for the L2 GRE tunnel service associated with the specified Virtual Private Network (VPN) ID.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is associated with the specified service.
- In addition to the virtual port configuration, this command also provides the status and additional configuration information for the service.
- Use the `isid` parameter to display debug information for the SPB service associated with the I-SID.
- Use the `vnid` parameter to display debug information for the VXLAN service associated with the VNID. This parameter is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
- Use the `vpnid` parameter to display debug information for the L2 GRE tunnel service associated with the VPNID.
Examples

-> show service 20 debug-info
Legend: (*): dyn unicast object (+): remote mcast object (#): local mcast object
SPB Service 20 Debug Info
Admin : Up, Oper : Down, Stats : N, Mtu : 9194, VLANXlation : N,
ISID : 1500, BVlan : 1500, MCast-Mode : Headend, Tx/Rx : 0/0,
VFI : 2, McIdx : 4094, StatsHandle : 0

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp FarEnd/Group</th>
<th>Intf</th>
<th>Sdp</th>
<th>Intf Name</th>
<th>VP</th>
<th>L2 McIdx</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/23:0</td>
<td>Down</td>
<td>Down</td>
<td>N</td>
<td></td>
<td>1/1/2</td>
<td>-</td>
<td></td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>sap:1/23:9.10</td>
<td>Down</td>
<td>Down</td>
<td>N</td>
<td></td>
<td>1/1/2</td>
<td>-</td>
<td></td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Total Ports: 2

-> show service 10 debug-info
Legend: (*): dyn unicast object (+): remote mcast object (#): local mcast object
VxLAN Service 10 Debug Info
Admin : Up, Oper : Down, Stats : N, VLANXlation : N,
VNID : 25000 (0.97.168), MCast-Mode : Hybrid,
VFI : 1, McIdx : 4095, StatsHandle : 0

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp FarEnd/Group</th>
<th>Intf</th>
<th>Sdp</th>
<th>Intf Name</th>
<th>VP</th>
<th>L2 McIdx</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/22:0</td>
<td>Up</td>
<td>Down</td>
<td>N</td>
<td></td>
<td>1/1/22</td>
<td>TOR-5</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>sap:1/22:all</td>
<td>Up</td>
<td>Down</td>
<td>N:0</td>
<td></td>
<td>1/1/22</td>
<td>-</td>
<td></td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>sap:1/22:2.5</td>
<td>Up</td>
<td>Down</td>
<td>N</td>
<td></td>
<td>1/1/22</td>
<td>-</td>
<td></td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

-> show service vpnid 200 debug-info
Legend: * denotes a dynamic object
L2GRE Service 20 (Guest)
Admin : Up, Oper : Up, Stats : N, VLANXlation : N,
VPNID : 200, RemoveIngTag: N,
VFI : 2, StatsHandle: 0

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Adm</th>
<th>Oper</th>
<th>Stats</th>
<th>Sdp FarEnd/Group</th>
<th>Intf</th>
<th>Sdp</th>
<th>Intf Name</th>
<th>VP</th>
<th>L2 McIdx</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/23:0</td>
<td>Up</td>
<td>Down</td>
<td>N</td>
<td></td>
<td>1/1/23</td>
<td>L2GRE-Loopack</td>
<td>3</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>sdp:200:20</td>
<td>Up</td>
<td>Up</td>
<td>Y</td>
<td></td>
<td>11.2.2.3</td>
<td>-</td>
<td>L2GRE-VPNID200</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Total Ports: 2

output definitions

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>The virtual ports (SAPs or SDPs) associated with the service.</td>
</tr>
<tr>
<td>Adm</td>
<td>The administrative state of the virtual port (Up or Down).</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational state of the virtual port (Up or Down).</td>
</tr>
<tr>
<td>Stats</td>
<td>Whether statistics collection is enabled for the virtual port.</td>
</tr>
<tr>
<td>Sap Trusted : Priority</td>
<td>Whether the Service Access Point (SAP) virtual port associated with the service is trusted or assigns a priority value.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sdp SystemId : BVlan</strong></td>
<td>The system ID (base MAC) and associated BVLAN for a Service Distribution Point (SDP) virtual port associated with the service. This value is displayed only for SPB services.</td>
</tr>
<tr>
<td><strong>Sdp FarEnd/Group</strong></td>
<td>The IP address (Loopback0 interface) or multicast group IP address associated with the far-end VXLAN node or the L2 GRE tunnel endpoint of this SDP. Note that L2 GRE SDPs only support far-end IP addresses. This value is displayed only for VXLAN and L2 GRE services.</td>
</tr>
<tr>
<td><strong>Intf</strong></td>
<td>The switch interface (port or link aggregate) of the virtual port (SAP or SDP) that is associated with the service.</td>
</tr>
<tr>
<td><strong>Sap Description</strong></td>
<td>The description for the SAP that is associated with the service.</td>
</tr>
<tr>
<td><strong>Sdp Systemname</strong></td>
<td>The system name for the SDP bridge that is associated with the service. This value is displayed only for SPB services.</td>
</tr>
<tr>
<td><strong>Sdp Intf Name</strong></td>
<td>The name assigned to the VXLAN or L2 GRE tunnel interface. This value is displayed only for VXLAN and L2 GRE services.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.
Release 7.3.4; **vnid** parameter and display fields added for VXLAN.
Release 8.4.1.R02; **vpnid** parameter and display fields added for L2 GRE.

Related Commands

- **show service ports** Displays the virtual port (SAP and SDP) configuration for the specified service.
- **show service** Displays the service configuration for the bridge.
- **show service access** Displays the service access port configuration for the switch.

MIB Objects

N/A
show service info

Displays the Service Manager configuration for the local switch.

show service info

**Syntax Definitions**

N/A

**Defaults**

By default, the UDP port value is set to 4789.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The display output of this command also includes SPB and VXLAN information, such as the system MAC address and name used by SPB and the UDP port and VRF used by VXLAN.
- Layer 2 Generic Routing Encapsulation (L2 GRE) information is displayed based on the switch platform. For example, the status of automatic discovery and the reserved VLAN ID is displayed only on those switches that support that functionality.

**Examples**

-> show service info

Service Manager System Info

SPB System Id : 00e0.b1e7.09a3,       SPB System Name : OS6860,
Service Trap  : Disable,              SAP Trap        : Disable,
SDP Trap      : Disable,              Bind Trap        : Disable,
Trap Rate Per Min: 60,                  VRRP TCAM Rule   : Enable,
Stats Admin State: Enable,              Stats Owner      : SvcMgr,
VxLAN Udp Port : 4789,                  VxLAN Current VRF: Default,
SDP auto-create : Enable

Sample output on an OmniSwitch 6560:

-> show service info

Service Manager System Info

SPB System Id : 2cfa.a2a2.e93f,       SPB System Name : OS6560,
Service Trap  : Disable,              SAP Trap        : Disable,
SDP Trap      : Disable,              Bind Trap        : Disable,
Service Manager Commands

show service info

---

| Trap Rate Per Min: 60, | VRRP TCAM Rule : Enable, |
| Stats Admin State: Disable, | Stats Owner : Available, |
| VxLAN Udp Port : 4789, | VxLAN Current VRF: Default, |
| L2GRE Rsvd VLAN : 4000, 4005, 4006, 4007, 4008, 4015, 4016, 4017 |

output definitions

| SPB System Id | The base MAC address of the local switch. |
| SPB System Name | The system name associated with the local switch. |
| Service Trap | The status (Enable or Disable) of trap generation for service status changes. |
| SAP Trap | The status (Enable or Disable) of trap generation for SAP status changes. |
| SDP Trap | The status (Enable or Disable) of trap generation for SDP status changes. |
| Bind Trap | The status (Enable or Disable) of trap generation for service bind status changes. |
| Trap Rate Per Min | The maximum number of traps that can be sent per minute. |
| VRRP TCAM Rule | The status (Enable or Disable) of how the switch processes VRRP packets (destination VRRP MAC address) received on access ports. When enabled, the customer VLAN tag is removed from VRRP packets. When disabled, the customer VLAN tag is not removed from VRRP packets. Configured through the service local-vrrp command. |
| Stats Admin State | The administrative status (Enable or Disable) of the statistics collection function. Configured through the service stats command. |
| Stats Owner | The system application in control of statistics collection. |
| VxLAN Udp Port | The UDP destination port for the Virtual eXtensible Local Area Network (VXLAN) feature. Configured through the service vxlan udp-port command. |
| VxLAN Current VRF | The name of the VRF instance for the VXLAN feature. Configured through the service vxlan vrf command. |
| Mgmt Change | The date and time of the last administrative status change. |
| Status Change | The date and time of the last operational status change. |
| SDP auto-create | The status (Enable or Disable) of automatic edge switch discovery on an L2 GRE tunnel aggregation switch. Configured through the service l2gre auto-discover command. Supported only on the OmniSwitch 6860, OmniSwitch 6865, OmniSwitch 6900, and OmniSwitch 9900. |
| L2GRE Rsvd VLAN | The reserved VLAN IDs for L2 GRE tunnel services. Configured through the service l2gre reserved-vlan command Supported only on the OmniSwitch 6560. |

Release History

Release 7.3.4; command was introduced; VXLAN fields added.
Release 8.3.1.R02; VRRP TCAM Rule field added.
Release 8.5R2; L2GRE auto-disc and L2GRE Rsvd VLAN fields added for L2 GRE tunnel services.
Release 8.5R4; **L2GRE auto-disc** field name changed to **SDP auto-create**.
Release 8.6R1; **L2GRE Rsvd VLAN** field allows display of multiple L2 GRE reserved VLANs.

**Related Commands**

*show service*  
Displays information about the services configured on the switch.

**MIB Objects**

alaSvcMgrSysTable
  alaSvcMgrSysId
  alaSvcMgrSysName
  alaSvcMgrSysLastMgmtChange
  alaSvcMgrSysLastStatusChange
  alaSvcMgrSvcTrapAdminState
  alaSvcMgrSapTrapAdminState
  alaSvcMgrSdpTrapAdminState
  alaSvcMgrSdpBindTrapAdminState
  alaSvcMgrMaxTrapPerMinute
  alaSvcMgrVrrpMacTcamRuleAdminState
  alaSvcMgrVxlanDestUdpPort
  alaSvcMgrVxlanVrfName
  alaSvcMgrSdpAutoCreateAdminState
  alaSvcMgrReservedL2greVlan
**show service l3vpn profile**

Displays the status of IP over SPB inline routing support. For more information about inline routing, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>In-use</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C6/T48C6/X48C4E</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Support for IP over SPB inline routing is enabled by default (Basic mode is active).
- When disabled (Basic mode is not active), inline routing cannot be configured on the switch, however, more system resources are available for other non-inline routing functionality (such as an increase in the number of Layer 3 interfaces, ARPs, etc.).

**Examples**

```
-> show service l3vpn profile
Legend: (*)In-use
Profile Name  L3 Intf  Next Hops  Ecmp Groups  Ecmp Members
-----------------------------------------------+
Basic*        1024     4096      256          1024
```

After inline routing support is disabled (no service l3vpn profile) and the switch is rebooted, the following is displayed:

```
-> show service l3vpn profile
Legend: (*)In-use
Profile Name  L3 Intf  Next Hops  Ecmp Groups  Ecmp Members
-----------------------------------------------+
Disabled*     0         0         0            0
```
**Release History**

Release 8.7R2; command was introduced.

**Related Commands**

- **service l3vpn profile**  
  Configures the status of IP over SPB inline routing support.

**MIB Objects**

- `alaCapManServiceL3vpnConfig`
- `alaCapManServiceL3vpn`
**show service counters**

Displays the traffic statistics for the specified service and associated virtual ports. A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is bound to the specified service.

```
show service {service_id | spb service_id | vnid vxlan_id | vpnid vpn_id} counters
```

### Syntax Definitions

- **service_id**: An existing service ID number.
- **vxlan_id**: Displays statistics for the VXLAN service associated with the specified VXLAN network identifier (VNID). The valid range is 1–16777215 (or 000.000.001–255.255.255 in dot-decimal notation format).
- **vpn_id**: Displays statistics for the L2 GRE tunnel service associated with the specified Virtual Private Network (VPN) ID.

### Defaults

N/A

### Platforms Supported

Not supported in this release.

### Usage Guidelines

- Enter an existing service ID number to display statistics for a specific service.
- Use the **vnid** parameter to display statistics for a specific VXLAN network identifier. A VNID identifies a specific VXLAN network segment. This parameter is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
- Use the **vpnid** parameter to display statistics for a specific L2 GRE VPN segment.

### Examples

```
-> show service 20 counters
Legend: * denotes a dynamic object

<table>
<thead>
<tr>
<th>Identifier</th>
<th>IngPkts</th>
<th>IngByteCount</th>
<th>EgrPkts</th>
<th>EgrByteCount</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1:10</td>
<td>1234</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sap:1/1:15</td>
<td>1234</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sap:8/2</td>
<td>1234</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sap:2/3:20.25*</td>
<td>1234</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sdp:32768:100</td>
<td>34</td>
<td>5678</td>
<td>4321</td>
<td>12345678</td>
</tr>
</tbody>
</table>
```
`-> show service vnid 1000 counters
Legend: * denotes a dynamic object

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Ing Pkts</th>
<th>Ing Byte Count</th>
<th>Egr Pkts</th>
<th>Egr Byte Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/5:20</td>
<td>1200</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sap:2/10:30.35*</td>
<td>1200</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sdp:32769:200</td>
<td>60</td>
<td>5678</td>
<td>4321</td>
<td>12345678</td>
</tr>
</tbody>
</table>

`-> show service vpnid 200 counters
Legend: * denotes a dynamic object

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Ing Pkts</th>
<th>Ing Byte Count</th>
<th>Egr Pkts</th>
<th>Egr Byte Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/23:10</td>
<td>1200</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sap:1/1/24:0</td>
<td>1200</td>
<td>12345678</td>
<td>12</td>
<td>123</td>
</tr>
<tr>
<td>sdp:200:20</td>
<td>60</td>
<td>5678</td>
<td>4321</td>
<td>12345678</td>
</tr>
</tbody>
</table>

**output definitions**

- **Identifier**: The virtual ports (SAPs or SDPs) associated with the service.
- **Ing Pkts**: The number of packets received on the virtual port.
- **Ing Byte Count**: The ingress packet byte count for the virtual port.
- **Egr Pkts**: The number of packets sent on the virtual port.
- **Egr Byte Count**: The egress packet byte count for the virtual port.

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.4; vnid parameter added for VXLAN.
Release 8.4.1.R02; vpnid parameter added for L2 GRE.

**Related Commands**

- **show service**: Displays the service configuration for the bridge.
- **show service ports**: Displays the virtual ports associated with the specified service.
- **clear service counters**: Clears the traffic statistics for the specified service and associated virtual ports.

**MIB Objects**

alaSvcBaseInfoTable
  - alaSvcIngressPacketCount
  - alaSvcIngressByteCount
  - alaSvcEgressPacketCount
  - alaSvcEgressByteCount
clear service counters

Clears the traffic statistics for the specified service and associated virtual ports. A virtual port represents a Service Access Point (SAP) or a Service Distribution Point (SDP) that is bound to the specified service.

```
clear service [service_id] [sap {port chassis/slot/port | linkagg agg_id]} :0 | :all | :qtag | :outer_qtag.inner_qtag] [mesh-sdp sdp_id] counters
```

**Syntax Definitions**

- `service_id`: An existing SPB service ID number.
- `chassis`: The chassis identifier.
- `slot/port`: The slot and port number of the service access port.
- `agg_id`: The link aggregate ID number (0–31) of a service access link aggregate.
- `:0`: Specifies a null encapsulation value for the SAP. Only untagged traffic is mapped to this SAP.
- `:all`: Specifies a wild-card SAP. All tagged traffic that is not classified into another SAP is mapped to the wild-card SAP.
- `:qtag`: Specifies a VLAN ID tag for traffic that ingresses on the access port. Only traffic with this tag is mapped to this SAP.
- `:outer_qtag.inner_qtag`: Specifies an outer VLAN ID tag and an inner VLAN tag for traffic that ingresses on the access port. Only double-tagged (QinQ) traffic with the specified outer and inner tags is mapped to this SAP.
- `sdp_id`: An existing mesh SDP ID.

**Defaults**

By default, all statistics counters for the specified service are cleared.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `sap` parameter options with this command to clear the statistics for a specific SAP ID. A SAP ID is comprised of an access port (`slot/port or agg_id`) and an encapsulation value (`:0, :all, :qtag, or :outer_qtag.inner_qtag`) that is used to identify the type of customer traffic to map to the associated service.

- Use the `mesh-sdp sdp_id` parameter to clear the statistics for a specific mesh SDP.
Examples

-> clear service counters  
-> clear service 100 counters  
-> clear service sap 8/2:all counters  
-> clear service mesh-sdp counters

Release History

Release 7.3.1; command was introduced.  
Release 7.3.4; VXLAN service support added.

Related Commands

show service counters Displays the traffic statistics for the specified SPB service and associated virtual ports.

MIB Objects

alaSvcBaseInfoTable  
   alaSvcClearCounters  
alaSapBaseInfoTable  
   alaSapClearCounters
**show service rfp**

Displays the configuration and status of SPB Remote Fault Propagation (RFP) domains.

```
show service rfp [rfp_id [local-sap-status]]
```

### Syntax Definitions

- **rfp_id**
  - An existing RFP ID number.

- **local-sap-status**
  - Displays information about the local SPB service elements that are bound to the specified RFP ID.

### Defaults

By default, information for all RFP domains is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter an existing RFP ID number to display statistics for a specific RFP domain.
- Use the **local-sap-status** parameter to display SPB service information for the specified RFP ID.

### Examples

```
-> show service rfp

Local system (Name: SystemId) = bridge1 : E8:E7:32:B8:9C:98
Total number of services information =6
Total Number of RFP domain =2
RFP  Remote  RMEP  System                  B-VLAN  ISID  Service  Admin
   EndPoint Status (Name: SystemId)  Id      State
-----------------------------------+---------+--------+---------+---------+---------+---------+---------+---------+
   1000   2  RMEP_OK  bridge2:E8:E7:32:B8:9C:95  4001  10000   10     Enable
   1000   3  RMEP_OK  bridge3:E8:E7:32:B8:9C:90  4002  20000   20     Enable
   1000   4  RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4003  30000   30     Enable
   2000   4  RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4004  40000   40     Enable
   2000   4  RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4005  50000   50     Enable
   2000   4  RMEP_OK  bridge4:E8:E7:32:B8:9C:88  4006  60000   60     Enable

-> show service rfp 1000

Local system (Name: SystemId) = bridge1 : E8:E7:32:B8:9C:98
Total number of services information =6
```
Total Number of RFP domain = 2

<table>
<thead>
<tr>
<th>RFP</th>
<th>Remote EndPoint Status</th>
<th>System (Name: SystemId)</th>
<th>B-VLAN</th>
<th>ISID</th>
<th>Service Id</th>
<th>Admin State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>RMEP_OK</td>
<td>bridge2:E8:E7:32:B8:9C:95</td>
<td>4001</td>
<td>10000</td>
<td>10</td>
<td>Enable</td>
</tr>
<tr>
<td>1000</td>
<td>RMEP_OK</td>
<td>bridge3:E8:E7:32:B8:9C:90</td>
<td>4002</td>
<td>20000</td>
<td>20</td>
<td>Enable</td>
</tr>
<tr>
<td>1000</td>
<td>RMEP_OK</td>
<td>bridge4:E8:E7:32:B8:9C:88</td>
<td>4003</td>
<td>30000</td>
<td>30</td>
<td>Enable</td>
</tr>
</tbody>
</table>

**output definitions**

**RFP**
The RFP ID number. Configured through the `service rfp local-endpoint` command.

**Remote EndPoint**
The ID number for the RFP remote end point. Configured through the `service rfp remote-endpoint` command.

**RMEP Status**
The status of the remote Maintenance End Point (MEP).

**System (Name: SystemId)**
The name and bridge MAC address of the remote SPB switch.

**B-VLAN**
The SPB backbone VLAN that serves as the primary VLAN for the RFP domain. The SPB control BVLAN is automatically used for each RFP OAM domain.

**ISID**
The SPB service instance ID. The ISID is bound to an SPB service ID, which in turn is bound to an SPB access port. This binding creates a Service Access Point (SAP), which is configured through the `service sap` command.

**Service Id**
An SPB service ID number. Configured through the `service spb` command and associated with the RFP ID through the `service rfp remote-endpoint` command.

**Admin State**
The administrative status (Enable or Disable) of the SAP port on the local chassis.

```
-> show service rfp 1000 local-sap-status

Local endpoint ID = 10
Local system (Name: SystemId) = bridge1: E8:E7:32:B8:9C:98

<table>
<thead>
<tr>
<th>Service Sap Id</th>
<th>Admin</th>
<th>Oper</th>
<th>Remote EndPoint Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/11:10</td>
<td>Enable</td>
<td>Up</td>
<td>2</td>
</tr>
<tr>
<td>sap:1/10:10</td>
<td>Enable</td>
<td>Up</td>
<td>3</td>
</tr>
<tr>
<td>sap:2/11:10</td>
<td>Enable</td>
<td>Violation</td>
<td>4</td>
</tr>
<tr>
<td>sap:2/12:10</td>
<td>Enable</td>
<td>Down</td>
<td>4</td>
</tr>
<tr>
<td>sap:2/13:10</td>
<td>Enable</td>
<td>Down</td>
<td>4</td>
</tr>
</tbody>
</table>
```

**Local endpoint ID**
The ID number of the local RFP end point.

**Local system (Name: SystemId)**
The name and bridge MAC address of the local SPB switch.

**Service Id**
An SPB service ID number. Configured through the `service spb` command and associated with the RFP ID through the `service rfp remote-endpoint` command.
show service rfp

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sap</td>
<td>The Service Access Point to which the SPB service ID is associated through the configured through the <code>service sap</code> command.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative status (<strong>Enable</strong> or <strong>Disable</strong>) of the SAP.</td>
</tr>
<tr>
<td>Oper</td>
<td>The operation status (<strong>Up</strong>, <strong>Down</strong>, <strong>Violation</strong>) of the SAP.</td>
</tr>
<tr>
<td>Remote EndPoint</td>
<td>The ID number for the RFP remote end point. Configured through the <code>service rfp remote-endpoint</code> command.</td>
</tr>
<tr>
<td>R-Endpoint Status</td>
<td>The status of the remote Maintenance End Point (MEP).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `show service rfp configuration` Displays the RFP OAM domain configuration for the bridge.

**MIB Objects**

- **N/A**
**show service rfp configuration**

Displays the RFP OAM domain configuration for the bridge. When an RFP domain is created, an Ethernet OAM domain is automatically configured on the switch and mapped to the RFP domain.

**show service rfp configuration [rfp_id]**

---

**Syntax Definitions**

*rfp_id* 
An existing RFP ID number.

**Defaults**

By default, information for all RFP OAM domains is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter an existing RFP ID number to display the OAM domain configuration for a specific RFM domain.
- For each RFP domain created, a separate OAM domain is also created and mapped to the RFP domain.

**Examples**

```
-> show service rfp configuration
Total Number of RFP domains - 2

RFP domain Number    : 1000
Admin status         : Enabled
Level                : 7
Type                 : SPB
Maintenance Domain   : RFP_OVER_SPB_DOMAIN_LEVEL7
Maintenance Association: RFP_OVER_SPB_ASSOCIATION
Control B-VLAN       : 1000
Virtual UP MEP ID    : 10
CCM interval         : 100 millisecond
Remote Endpoint service ID
-----------------------
1  10,11
2  20
3-9 40

RFP domain Number    : 2000
```
Admin status : Enabled
Level : 6
Type : SPB
Maintenance Domain : RFP_OVER_SPB_DOMAIN_LEVEL6
Maintenance Association: RFP_OVER_SPB_ASSOCIATION
Control B-VLAN : 1000
Virtual UP MEP ID : 10
CCM interval : 100 millisecond
Remote Endpoint service ID
---------------+----------
1             30,31
2             50
3-9           70

-> show service rfp configuration 1000

RFP domain Number : 1000
Admin status : Enabled
Level : 7
Type : SPB
Maintenance Domain : RFP_OVER_SPB_DOMAIN_LEVEL7
Maintenance Association: RFP_OVER_SPB_ASSOCIATION
Control B-VLAN : 1000
Virtual UP MEP ID : 10
CCM interval : 100 millisecond
Remote Endpoint service ID
---------------+----------
1             10,11
2             20
3-9           40

output definitions

RFP domain number The RFP ID number, that is mapped to the OAM domain.
Admin State The administrative status (Enable or Disable) of the RFP domain.
Level The Maintenance Domain (MD) level.
Type The type of RFP domain (SPB is the only type currently supported).
Maintenance Domain The name of the reserved MD assigned to the RFP domain.
Maintenance Association The name of the Maintenance Association (MA) for the RFP (MD). The same MA name is used for all RFP domains.
Control B-VLAN The SPB control BVLAN that serves as the primary VLAN for the RFP OAM domain.
Virtual UP MEP ID The local end point ID for the RFP domain.
CCM interval The time interval at which a Continuity Check Message (CCM) is sent for this domain.
Remote Endpoint service ID The RFP ID number for the remote end point.

Release History

Release 7.3.4; command was introduced.
Related Commands

show service rfp

Displays the configuration and status of SPB Remote Fault Propagation (RFP) domains.

MIB Objects

N/A
11 Loopback Detection Commands

Loopback Detection (LBD) automatically detects the loop and shutdown the port involved in the loop. This prevents forwarding loops on ports that have forwarded network traffic which has looped back to the originating switch. LBD detects and prevents Layer 2 forwarding loops on a port either in the absence of other loop detection mechanisms such as STP/RSTP/MSTP, or when these mechanisms cannot detect it (for example, a client's equipment may drop BPDUs, or the STP protocol may be restricted to the network edge). On a linkagg port, if one port of linkagg is getting shutdown due to LBD, then all the ports of linkagg will go to shutdown state.

Loopback Detection is enabled system wide and on a per-port basis. Once a loop is discovered, the port from which the loop originated is placed into an “Inactive” state and when the two ports of a switch is connected to each other through a hub, either the ports will be shutdown or it will be in normal state.

A provider network with a set of multiple switches interconnected together can be logically viewed as a large single switch. The large single switch provides service access points to customers' networks. Configuration faults in customer networks can result in loops spanning both provider and customer networks. This can result in broadcast storms. In order to protect provider's network from broadcast storms, loops that involve SAP ports need to be detected and broken.

The LBD can detect and break loops created on the service-access interface.

For a service-access interface, LBD can be enabled for a specific port or linkagg. LBD for service-access points allows shutting down only the specific interface of the link involved in the loop.

When loopback occurs, a trap is sent and the event is logged. The port which is shutdown due to LBD is automatically recovered if autorecovery-timer is set or the port can manually be enabled again when the problem is resolved.

MIB information for the Loopback Detection commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>ALCATEL-IND1-LBD-MIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>alcatelIND1LBDMIB</td>
</tr>
</tbody>
</table>

A summary of available commands is listed here:

```
loopback-detection
loopback-detection port
loopback-detection service-access
loopback-detection transmission-timer
loopback-detection autorecovery-timer
show loopback-detection
show loopback-detection port
show loopback-detection linkagg
show loopback-detection statistics port
clear loopback-detection statistics port
```
loopback-detection

Enables or disables Loopback Detection (LBD) or remote origin LBD globally on the switch.

`loopback-detection [remote-origin] {enable | disable}`

**Syntax Definitions**

| enable | Disables LBD on the switch. |
| disable | Enables LBD on the switch. |

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- LBD can be enabled globally and per port without any dependency but `loopback-detection` will be operational only if LBD is enabled globally and also on the specific port.

- LBD can be configured for a port and the configuration can be applied and retained, whether or not LBD is enabled globally. However, LBD functionality on a port is available only when LBD is enabled globally on the switch.

- Enabling the `remote-origin` LBD option allows the switch to process the LBD frames originated from a remote system. The port from which the LBD frames originated will be shut down.

**Examples**

- `-> loopback-detection enable`
- `-> loopback-detection disable`
- `-> loopback-detection remote-origin enable`
- `-> loopback-detection remote-origin disable`

**Release History**

Release 7.3.4; command was introduced.
Release 8.2.1; `remote-origin` parameter added.
**Related Commands**

- `loopback-detection port` Enables or disables LBD on a specific port.
- `show loopback-detection` Displays LBD configuration information.

**MIB Objects**

- `alaLbdGlobalConfigStatus`
- `alaLbdGlobalRemoteConfigStatus`
**loopback-detection port**

Enables or disables LBD or remote-origin LBD on a specific bridge port.

`loopback-detection port chassis/slot/port[-port2] [remote-origin] {enable | disable}`

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **enable**
  - Enables LBD on the specified port.

- **disable**
  - Disables LBD on the specified port.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>chassis</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Loopback Detection must be enabled globally to enable LBD functionality on a specific port.
- For per-port remote origin LBD to work, both LBD and remote origin LBD must be enabled globally.
- LBD can be configured for a port and the configuration can be applied and retained, whether or not LBD is enabled globally. However, LBD functionality on a port is available only when LBD is enabled globally on the switch.
- When a LBD port joins a link aggregate, the LBD configuration on the joined port is removed.

### Examples

```
-> loopback-detection port 1/1/1 enable
-> loopback-detection port 1/1/1-8 enable
-> loopback-detection port 1/1/2 remote-origin enable
-> loopback-detection port 1/1/3-5 remote-origin enable
-> loopback-detection port 1/1/2 remote-origin disable
-> loopback-detection port 1/1/3-5 remote-origin disable
```
**Release History**

Release 7.3.4; command was introduced.
Release 8.2.1; `remote-origin` parameter added.

**Related Commands**

- `loopback-detection` Enables or disables LBD globally on the switch.
- `show loopback-detection` Displays LBD configuration information.
- `show loopback-detection port` Displays LBD port configuration information.

**MIB Objects**

- `alaLbdPortConfigTable`
  - `alaLbdPortConfigEntry`
  - `alaLbdPortConfigIndex`
  - `alaLbdPortConfigLbdAdminStatus`
  - `alaLbdPortConfigLbdOperStatus`
  - `alaLbdPortRemoteConfigAdminStatus`
**loopback-detection service-access**

Enables or disables LBD on a specific service access port or link aggregate or on a range of ports or link aggregates. When enabled, LBD can detect and break loops created on a service access interface.

`loopback-detection service-access {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} {enable | disable}`

### Syntax Definitions

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `enable` Enables LBD on the specified port or linkagg.
- `disable` Disables LBD on the specified port or linkagg.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Before configuring LBD using the `service-access` option, the port or linkagg must be configured for service access. Use the `service access` command to configure the port or linkagg for service access.

- The `service-access` option allows shutting down only the specific interface of the link involved in the loop.

- The linkagg must be formed by ports with same path cost.

- LBD is applicable on a linkagg only if the linkagg is configured as a service access interface.

- LBD cannot be configured on a linkagg that has member ports running LBD configuration and vice versa.

- When a linkagg is in violation or shutdown state, the member ports cannot be deleted from the linkagg.
Examples

-> loopback-detection service-access port 1/1/1 enable
-> loopback-detection service-access port 1/1/1-8 enable
-> loopback-detection service-access linkagg 1 enable

Release History

Release 7.3.4; command was introduced.

Related Commands

- `loopback-detection` Enables or disables LBD globally on the switch.
- `show loopback-detection` Displays LBD configuration information.
- `show loopback-detection port` Displays LBD port configuration information.
- `show loopback-detection linkagg` Displays LBD configuration information for a service access link aggregate.

MIB Objects

alaLdbPortConfigTable
  alaLdbPortConfigLdbAdminStatus
  alaLbdUserPortConfigLbdInterfaceType
Loopback Detection Commands

**loopback-detection transmission-timer**

Configures the LBD transmission timer on the switch. The transmission time is the time period between the consecutive LBD packet transmissions.

`loopback-detection transmission-timer seconds`

---

**Syntax Definitions**

- `seconds` The time period in seconds between LBD packet transmissions. The valid range is from 5 to 600 seconds.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- If the timer value is not configured, the default value of 30 seconds is assigned to the transmission period.
- The timer can be modified at any time. However, the new timer value will come into effect only after the timer is restarted.

**Examples**

```
-> loopback-detection transmission-timer 200
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- **loopback-detection**
  Enables or disables LBD globally on the switch.

- **show loopback-detection**
  Displays LBD configuration information.

MIB Objects

- **alaLbdGLocalConfigTransmissionTimer**
**loopback-detection autorecovery-timer**

Configures the LBD autorecovery timer on the switch. The autorecovery time is the time period in which the switch is recovered from the shutdown state.

**loopback-detection autorecovery-timer** seconds

---

**Syntax Definitions**

seconds The time period in seconds in which the switch is recovered from the shutdown state. The valid range is from 30 to 86400 seconds.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>300</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- If the timer value is not configured, the default value of 300 seconds is assigned to the autorecovery period.
- The timer can be modified at any time. However, the new timer value will come into effect only after the timer is restarted.

---

**Examples**

```
-> loopback-detection autorecovery-timer 200
```

---

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- `loopback-detection` : Enables or disables LBD globally on the switch.
- `show loopback-detection` : Displays LBD configuration information.

MIB Objects

- `alaLbdGlobalConfigAutorecoveryTimer`
**show loopback-detection**

Displays the global LBD configuration information for the switch.

**show loopback-detection**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view information for a specific port or service access link aggregate, use the **show loopback-detection port** or **show loopback-detection linkagg** command.

**Examples**

```
-> show loopback-detection
Global LBD Status : enabled,
Global Remote-origin LBD Status : disabled,
Global LBD Transmission Timer : 30 sec,
Global LBD Auto-recovery Timer : 300 sec,
```

**output definitions**

- **Global LBD Status**: The current status of LBD of the switch (enabled or disabled).
- **Global Remote-origin LBD Status**: The current status of remote-origin LBD of the switch (enabled or disabled).
- **Global LBD Transmission Timer**: Displays the time interval in seconds between LBD packet transmissions.
- **Global LBD Auto-recovery Timer**: Displays the time in which the switch recovered from the shutdown state.
**Release History**

Release 7.3.4; command was introduced.
Release 8.2.1; “Global Remote-origin LBD Status” field added.

**Related Commands**

- `loopback-detection` Enables or disables LBD globally on the switch.
- `show loopback-detection port` Displays LBD configuration information for bridge and service access ports on the switch.
- `show loopback-detection linkagg` Displays LBD configuration information for a service access link aggregate.
- `show violation` Displays the administrative status, link status, violations, recovery time, maximum recovery attempts and the value of the wait-to-restore timer for the specified port or ports.

**MIB Objects**

- `alaLbdGlobalConfigStatus`
- `alaLbdGlobalRemoteConfigStatus`
- `alaLbdGlobalConfigTransmissionTimer`
- `alaLbdGlobalConfigAutorecoveryTimer`
show loopback-detection port

Displays the LBD configuration information for the specified bridge or service access port.

```
show loopback-detection port [chassis/slot/port]
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1).

**Defaults**

By default, the LBD configuration for all ports is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8C32E/T24C2</th>
<th>9900X48C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The command can be used only on an LBD enabled port.

- Use the `loopback-detection port` command to enable LBD on a bridge port.
- Use the `loopback-detection service-access` command to enable LBD on a service access port or link aggregate.

**Examples**

```
-> show loopback-detection port
Slot/Port  Admin State  Remote-origin Status  OperState     Time-to-recovery (sec)
---------------------------------------------------------------------------------------------------------
1/1/1      enabled     enabled       Remote ShutDown             -
1/1/2      enabled     -             Normal                      -
```

**output definitions**

- **Slot/Port**: The slot/port number of the LBD port.
- **Admin State**: The administrative state of the port (enabled or disabled).
- **Remote-origin Status**: The remote-origin LBD status of the port (enabled or disabled). This field does not apply to LBD service access ports.
- **OperState**: The operational state of the port (Normal or Inactive).
- **Time-to-recovery (sec)**: The amount of time to recovery during an LBD shutdown.
-> show loopback-detection port 1/1/1
Global LBD Status          : enabled,
Global Remote-origin LBD Status : enabled,
Global LBD Transmission Timer : 30 sec,
Global LBD Auto-recovery Timer : 300 sec,
Port LBD Status            : enabled,
Port Remote-origin LBD Status : enabled,
Port LBD State             : Remote ShutDown,
Remote Src Mac             : E8:E7:32:9A:5A:4E,
Remote BridgeId            : E8:E7:32:9A:5A:3F,
Port LBD Type              : normal-edge,

-> show loopback-detection port 1/1/2
Global LBD Status          : enabled,
Global Remote-origin LBD Status : disabled,
Global LBD Transmission Timer : 30 sec,
Global LBD Auto-recovery Timer : 300 sec,
Port LBD Status            : enabled,
Port Remote-origin LBD Status : -,
Port LBD State             : Inactive,
Port LBD Type              : service-edge,

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global LBD Status</td>
<td>The current status of LBD of the switch (enabled or disabled).</td>
</tr>
<tr>
<td>Global Remote-origin LBD Status</td>
<td>The current status of remote-origin LBD on the switch (enabled or disabled).</td>
</tr>
<tr>
<td>Global LBD Transmission Timer</td>
<td>Displays the time interval in seconds between LBD packet transmissions.</td>
</tr>
<tr>
<td>Global LBD Auto-recovery Timer</td>
<td>Displays the time interval in seconds in which the switch is recovered from the shut down state.</td>
</tr>
<tr>
<td>Port LBD Status</td>
<td>Displays the administrative status of the port.</td>
</tr>
<tr>
<td>Port Remote-origin LBD Status</td>
<td>Displays the remote-origin LBD status of the port (enabled or disabled). This field does not apply to LBD service access ports.</td>
</tr>
<tr>
<td>Port LBD State</td>
<td>Displays the current operational state of the port.</td>
</tr>
<tr>
<td>Remote Src Mac</td>
<td>Displays the MAC address of the remote system. The Remote Src Mac is displayed only if remote-origin LBD is enabled on the system.</td>
</tr>
<tr>
<td>Remote BridgeId</td>
<td>Displays the bridge ID of the remote system. The Remote BridgeId is displayed only if remote-origin LBD is enabled on the system.</td>
</tr>
<tr>
<td>Port LBD Type</td>
<td>Displays the type of the interface—whether a normal edge interface or a service access interface.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command was introduced.
Release 8.2.1; fields added to display LBD remote origin information.
**Related Commands**

- `loopback-detection` Enables or disables LBD globally on the switch.
- `loopback-detection port` Enables or disables LBD for a bridge port.
- `loopback-detection service-access` Enables or disables LBD for a service access port or link aggregate.
- `show loopback-detection linkagg` Displays LBD configuration information for a service access link aggregate.
- `show loopback-detection statistics port` Displays LBD statistics information for a specific port.

**MIB Objects**

- `alaLbdGlobalConfigStatus`
- `alaLbdGlobalRemoteConfigStatus`
- `alaLbdGlobalConfigTransmissionTimer`
- `alaLbdGlobalConfigAutorecoveryTimer`
- `alaLbdPortConfigTable`
- `alaLbdPortConfigLbdAdminStatus`
- `alaLbdPortConfigLbdOperStatus`
- `alaLbdPortConfigServiceAccessType`
- `alaLbdPortRemoteConfigAdminStatus`
- `alaLbdPortRemoteSrcMacAddr`
- `alaLbdPortRemoteBridgeID`
- `alaLbdPortTimeToRecovery`
show loopback-detection linkagg

Displays the LBD configuration information for the specified link aggregate ID.

show loopback-detection linkagg *agg_id*

**Syntax Definitions**

*agg_id* The link aggregate ID number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The command can be used only on an LBD enabled link aggregate. Use the `loopback-detection service-access` command to enable LBD on a service access link aggregate.

**Examples**

```
--> show loopback-detection linkagg 10
Global LBD Status : enabled,
Global Remote-origin LBD Status : disabled,
Global LBD Transmission Timer : 30 sec,
Global LBD Auto-recovery Timer : 300 sec,
Linkagg LBD Status : disabled,
Linkagg LBD State : Inactive,
Linkagg LBD Type : service-access
```

**output definitions**

- **Global LBD Status** The current LBD status for the switch (enabled or disabled).
- **Global Remote-origin LBD Status** The current status of remote-origin LBD on the switch (enabled or disabled). This field does not apply to LBD link aggregates.
- **Global LBD Transmission Timer** Displays the time interval in seconds between LBD packet transmissions.
- **Global LBD Auto-recovery Timer** Displays the time interval in seconds in which the switch is recovered from the shut down state.
- **Linkagg LBD Status** Displays the administrative status of the link aggregate.
output definitions (continued)

<table>
<thead>
<tr>
<th>Linkagg LBD State</th>
<th>Displays the current operational state of the link aggregate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linkagg LBD Type</td>
<td>Displays the type of the interface—whether a normal edge interface or a service access interface. LBD supported on service access link aggregates.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command was introduced.
Release 8.2.1; fields added to display LBD remote origin information.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loopback-detection</td>
<td>Enables or disables LBD globally on the switch.</td>
</tr>
<tr>
<td>loopback-detection service-access</td>
<td>Enables or disables LBD for a service access port or link aggregate.</td>
</tr>
<tr>
<td>show loopback-detection statistics port</td>
<td>Displays LBD statistics information for a specific port.</td>
</tr>
</tbody>
</table>

MIB Objects

- alaLbdGlobalConfigStatus
- alaLbdGlobalRemoteConfigStatus
- alaLbdGlobalConfigTransmissionTimer
- alaLbdGlobalConfigAutorecoveryTimer
- alaLbdPortConfigTable
  | alaLbdPortConfigLbdAdminStatus
  | alaLbdPortConfigLbdOperStatus
  | alaLbdPortConfigServiceAccessType
**show loopback-detection statistics port**

Displays LBD statistics information for a specific port on the switch.

**Syntax Definitions**

- **chassis**  
  The chassis identifier.

- **slot/port**  
  The slot and port number (3/1).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The link aggregate ID is not displayed if the link aggregate is operationally down.

**Examples**

```
-> show loopback-detection statistics port 1/1/1
LBD Port Statistics
LBD Packet Send    : 1,
Invalid LBD Packet Received : 0,
Member of Link Aggregation : -
```

```
-> show loopback-detection statistics port 1/1/3
LBD Port Statistics
LBD Packet Send    : 1,
Invalid LBD Packet Received : 0,
Member of Aggregation : 2
```

**output definitions**

- **LBD Packet Send**  
  The number of LBD packet sent from the port.

- **Invalid LBD Packet Received**  
  The number of invalid LBD packets received on the port.

- **Member of Aggregation**  
  The linkagg ID in which the port is a member.
Release History
Release 7.3.4; command was introduced.

Related Commands

**loopback-detection**  
Enables or disables LBD globally on the switch.

**show loopback-detection port**  
Displays LBD configuration information for a specific port.

MIB Objects

alaLbdPortStatsTable
- alaLbdPortStatsIfIndex
- alaLbdPortNumLbdInvalidRcvd
- alaLbdPortLbdSent
- alaLbdPortLinkAgg
clear loopback-detection statistics port

Clears statistics of all LBD ports or a specific port.

clear loopback-detection statistics port [chassis/slot/port]

**Syntax Definitions**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port</td>
<td>The slot and port number (3/1).</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> clear loopback-detection statistics port 1/1/2

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- **loopback-detection** Enables or disables LBD globally on the switch.
- **show loopback-detection port** Displays LBD configuration information for a specific port.

**MIB Objects**

alaLbdPortStatsTable
alaLbdPortStatsClear
Link aggregation combines multiple physical links between two switches into one logical link. The aggregate group operates within Spanning Tree as one virtual port and can provide more bandwidth than a single link. It also provides redundancy. If one physical link in the aggregate group goes down, link integrity is maintained.

There are two types of aggregate groups: static and dynamic. Static aggregate groups are manually configured on the switch with static links. Dynamic groups are set up on the switch but they aggregate links as necessary according to the Link Aggregation Control Protocol (LACP).

The dynamic aggregation software is compatible only with the following IEEE standard:

802.3ad — Aggregation of Multiple Link Segments

MIB information for the link aggregation commands is as follows:

Filename: ALCATEL-IND1-LAG-MIB.mib
Module: alcatelIND1LAGMIB
A summary of available commands is listed here:

| Static link aggregates                      | linkagg static agg size  |
|                                            | linkagg static agg name  |
|                                            | linkagg static agg wait-to-restore-time |
|                                            | linkagg static agg loopback |
|                                            | linkagg static agg loopback internal |
|                                            | linkagg static agg admin-state |
|                                            | linkagg static agg port agg |

| Dynamic link aggregates                     | linkagg lacp agg size     |
|                                            | linkagg lacp agg name      |
|                                            | linkagg lacp agg wait-to-restore-time |
|                                            | linkagg lacp agg admin-state |
|                                            | linkagg lacp agg actor admin-key |
|                                            | linkagg lacp agg actor system-priority |
|                                            | linkagg lacp agg actor system-id |
|                                            | linkagg lacp agg partner system-id |
|                                            | linkagg lacp agg partner system-priority |
|                                            | linkagg lacp agg partner admin-key |
|                                            | linkagg lacp port actor admin-key |
|                                            | linkagg lacp port admin-state |
|                                            | linkagg lacp port admin-state |
|                                            | linkagg lacp port actor system-id |
|                                            | linkagg lacp port actor system-priority |
|                                            | linkagg lacp port admin-state |
|                                            | linkagg lacp port partner admin system-id |
|                                            | linkagg lacp port partner admin-key |
|                                            | linkagg lacp port partner admin system-priority |
|                                            | linkagg lacp port actor port priority |
|                                            | linkagg lacp port partner admin-port |
|                                            | linkagg lacp port partner admin port-priority |

| Dual Home Link (DHL)                         | dhl name                  |
| Active-Active                                 | dhl linka linkb            |
|                                            | dhl admin-state           |
|                                            | dhl vlan-map linkb        |
|                                            | dhl pre-emption-time      |
|                                            | dhl mac-flushing          |
|                                            | show dhl                  |
|                                            | show dhl link              |

| Static and dynamic                           | show linkagg              |
|                                            | show linkagg port         |
|                                            | show linkagg accounting   |
|                                            | show linkagg counters     |
|                                            | show linkagg traffic      |
|                                            | clear linkagg-statistics  |
**linkagg static agg size**

Creates a static aggregate group between two switches. A static aggregate group contains static links.

```
linkagg static agg agg_id[-agg_id2] size size [name name] [admin-state {enable | disable}] [multi-chassis active] [hash {source-mac | destination-mac | source-and-destination-mac | source-ip | destination-ip | source-and-destination-ip | tunnel-protocol}]
```

```
no linkagg static agg agg_id[-agg_id2]
```

**Syntax Definitions**

- `agg_id[-agg_id2]` The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `size` The maximum number of links allowed in the aggregate group.
- `name` The name of the static aggregate group. Can be any alphanumeric string. A group name with spaces must be contained within quotes (for example, “Static Group 1”).
- `enable` Specifies that the static aggregate group is active and is able to aggregate links.
- `disable` Specifies that the static aggregate group is inactive and not able to aggregate links.
- `multi-chassis active` This parameter is not supported.
- `source-mac` Selects the source MAC address hashing option.
- `destination-mac` Selects the destination MAC address hashing option.
- `source-and-destination-mac` Selects the source MAC address and destination MAC address hashing option.
- `source-ip` Selects the source IP hashing option.
- `destination-ip` Selects the destination IP hashing option.
- `source-and-destination-ip` Selects the source IP and destination IP hashing option.
- `tunnel-protocol` Selects the tunnel protocol (payload based) hashing option.
### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td><em>hash_option</em></td>
<td>source-and-destination-IP (Layer 3 traffic)</td>
</tr>
<tr>
<td></td>
<td>source-and-destination-mac (Layer 2 traffic)</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove a static aggregate group or a range of static aggregate groups from the configuration.

- Link aggregation cannot be configured on an AppMon enabled port.

- If the static aggregate has any attached ports, delete the attached ports with the `no` form of the `linkagg static port agg` command then remove the static link aggregate ID. Delete the attached ports using the `no linkagg static port` command.

- Specify the `hash` parameter option when the link aggregate is first created. The hashing algorithm options apply to unicast traffic and are not modifiable once the aggregate is created. If different options are required:
  - Disassociate all ports currently associated with the aggregate.
  - Delete the aggregate from the switch configuration.
  - Create the aggregate again with the new hashing options.

- It is not necessary to administratively down the linkagg ports before changing the hashing algorithm, but doing so is recommended to avoid any loss of traffic.

- The hashing algorithm does not take into consideration the speed of the ports to distribute the traffic. In other words, the same number of flows is distributed evenly on each port without consideration of the line speed.

- Aggregate load balancing is performed at the ingress side.

- Per-aggregate hashing is local to the switch, so each side of the aggregation can use different configurations for the hashing algorithms.

- Link aggregation follows the global hash control settings configured through the `hash-control brief` or `hash-control extended` commands.
For example, when the **source-mac** option is specified for L2 hashing:
- If the global hash-control is in brief mode, hashing is based on source MAC address only.
- If the global hash-control is in extended mode, hashing is based on source MAC address, VLAN, Ethertype, and source module ID/port.

For example, when the **source-ip** option is specified for L3 hashing:
- If the global hash-control is in brief mode, hashing is based on source IP address only.
- If the global hash-control is in extended mode, hashing is based on source IP address and source UDP-TCP Port.

To load balance Unknown Destination/Broadcast/Multicast traffic on all the ports of the aggregate, use the **hash-control** command to enable load balancing of DFL traffic.

Use the **linkagg lacp agg size** command to create a dynamic aggregation (LACP) group.

### Examples

```
-> linkagg static agg 3-10 size 8
-> linkagg static agg 4 size 2 admin-state disable
-> linkagg static agg 4 size 2 hash source-and-destination-ip
-> no linkagg static agg 3-10
```

### Release History

- Release 7.1.1; command introduced.
- Release 7.3.1; **tunnel-protocol** parameter added.

### Related Commands

**show linkagg**

Displays information about static and dynamic (LACP) link aggregate groups.

### MIB Objects

**alclnkaggAggTable**

- **alclnkaggAggNumber**
- **alclnkaggAggSize**
- **alclnkaggAggLacpType**
- **alclnkaggAggName**
- **alclnkaggAggAdminState**
- **alclnkaggAggPortSelectionHash**
**linkagg static agg name**

Configures a name for an existing static aggregate group.

```
linkagg static agg agg_id[{-agg_id2}] name name
no linkagg static agg agg_id[{-agg_id2}] name
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>agg_id[{-agg_id2}]</code></td>
<td>The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).</td>
</tr>
<tr>
<td><code>name</code></td>
<td>The name of the static aggregation group, can be an alphanumeric string. A group name with spaces must be contained within quotes (for example, “Static Group 1”)</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a name from a static aggregate or from a range of static aggregates.
- You must assign names to static link aggregate IDs individually.
- To specify a range of link aggregates, use hyphen between the first and last link aggregate IDs of the range. A range of link aggregate IDs can be used only with the **no** form of this command.

**Examples**

```
-> linkagg static agg 2 name accounting
-> no linkagg static agg 2-10 name
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

**linkagg static agg size**
Creates a static aggregate group.

**show linkagg**
Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

```
alclnkaggAggTable
    alclnkaggAggNumber
    alclnkaggAggName
```
linkagg static agg wait-to-restore-time

Configures the number of minutes to wait before bringing up a link aggregate that is attached to other link aggregates.

linkagg static agg agg_id[-agg_id2] wait-to-restore-time wtr_minutes

no linkagg static agg agg_id[-agg_id2] wait-to-restore-time

Syntax Definitions

agg_id[-agg_id2] The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

wtr_minutes The number of minutes the switch waits to bring a link aggregate up. The range is 0–12 minutes.

Defaults

By default, the wait-to-restore timer is set to 0 (disabled).

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable the wait-to-restore timer for the specified link aggregate or aggregates.

- If a link aggregate is not attached to other links, this timer value is ignored and the aggregate is immediately brought up.

Examples

- `-> linkagg static agg 2 wait-to-restore-time 10`
- `-> linkagg static agg 2 wait-to-restore-time 0`
- `-> linkagg static agg 4 wait-to-restore-time 5`
- `-> no linkagg static agg 4 wait-to-restore-time`

Release History

Release 7.1.1; command introduced.
Related Commands

- `linkagg static agg size`  Creates a static aggregate group.
- `show linkagg`  Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

- `alclnkaggAggTable`
  - `alclnkaggAggNumber`
  - `alclnkaggAggWTRTimer`
**linkagg static agg loopback**

Configures the specified link aggregate group to run in loopback mode. This is required if the link aggregate is going to provide loopback functionality to support L3 VPN in-line routing for an IP over Shortest Path Bridging (SPB) configuration.

**Syntax Definitions**

`agg_id[agg_id2]` An existing link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Only front-panel ports that are also configured to run in loopback mode can be assigned to this type of link aggregate.

- Once the loopback mode is enabled for a link aggregate, the link aggregate is dedicated to providing loopback functionality for an SPB L3 VPN in-line routing configuration. The loopback mode is disabled only when the link aggregate is deleted.

- For more information about SPB L3 VPN, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

**Examples**

- `-> linkagg static agg 2 loopback`
- `-> linkagg static agg 10 loopback`

**Release History**

Release 8.6R2; command introduced.
**Related Commands**

- `linkagg static agg size` Creates a static aggregate group.
- `interfaces loopback` Configures a front-panel port to run in the loopback mode.
- `show linkagg` Displays information about static and dynamic (LACP) aggregate groups.

**MIB Objects**

- `alclnkaggAggTable`
  - `alclnkaggAggNumber`
  - `alclnkaggAggLoopbackState`
linkagg static agg loopback internal

Configures the specified link aggregate group to run in internal loopback mode. This is required if the link aggregate is going to provide loopback functionality to support L3 VPN inline routing for an IP over Shortest Path Bridging (SPB) configuration.

**linkagg static agg **agg_id[-agg_id2] loopback

**Syntax Definitions**

agg_id[-agg_id2] An existing link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- When the internal loopback mode is enabled, internal ports are assigned to the link aggregate group. These ports are dedicated for this purpose; front-panel ports are not assigned to this type of link aggregate.
- No external cable is required and no front-panel ports are used up to provide the L3 VPN loopback functionality when internal loopback is used to define an L3 VPN gateway interface.
- Only one link aggregate per switch can be configured to run in the internal loopback mode.
- Once the internal loopback mode is enabled for a link aggregate, the link aggregate is dedicated to providing loopback functionality for an SPB L3 VPN inline routing configuration. The internal loopback mode is disabled only when the link aggregate is deleted.
- For more information about SPB L3 VPN, see the “IP over SPBM” section of the “Configuring Shortest Path Bridging” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide.

**Examples**

-> linkagg static agg 2 loopback internal
-> linkagg static agg 10 loopback internal
ERROR: Internal Loopback aggregate already exists

**Release History**

Release 8.6R2; command introduced.
Related Commands

**linkagg static agg size**

Creates a static aggregate group.

**show linkagg**

Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

alclnkaggAggTable
  alclnkaggAggNumber
  alclnkaggAggLoopbackState
**linkagg static agg admin-state**

Enables or disables the administrative state of a static link aggregation group.

```
linkagg static agg agg_id[-agg_id2] admin-state {enable | disable}
```

**Syntax Definitions**

- **agg_id[-agg_id2]**: The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).
- **enable**: Specifies that the static aggregate group is active and is able to aggregate links.
- **disable**: Specifies that the static aggregate group is inactive and not able to aggregate links.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the administrative state is set to **disable**, the static aggregate group is disabled.

**Examples**

```
→ linkagg static agg 2 admin-state disable
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

`linkagg static agg size`  Creates a static aggregate group.
`show linkagg`  Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

`alclnkaggAggTable`
- `alclnkaggAggNumber`
- `alclnkaggAggAdminState`
**linkagg static port agg**

Configures a slot and port for a static aggregate group.

```
linkagg static port chassis/slot/port[-port2] agg agg_id
no linkagg static port chassis/slot/port[-port2]
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
- **agg_id**: The ID number corresponding to the static aggregate group.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove one or more ports from a static aggregate group.
- A port can belong to only one aggregate group.
- Ports that belong to the same static aggregate group need not be configured sequentially and can be on any Network Interface (NI).
- To specify a range of link aggregates, use hyphen between the first and last link aggregate IDs of the range. A range of link aggregate IDs can be used only with the `no` form of this command.

**Examples**

```
-> linkagg static port 2/1-5 agg 4
-> no linkagg static port 2/1-5
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

`linkagg static agg size`  Creates a static aggregate group.
`show linkagg port`  Displays information about link aggregation ports.

MIB Objects

`alclnkaggAggPortTable`  
- `alclnkaggAggPortGlobalPortNumber`
- `alclnkaggAggPortLacpType`
- `alclnkaggAggPortSelectedAggNumber`
**linkagg lACP agg size**

Creates a dynamic aggregate group that uses the Link Aggregation Control Protocol (LACP) to establish and maintain link aggregation. The **size** parameter is required to create the link aggregate group.

```
linkagg lACP agg agg_id[-agg_id2] size size
   [name name]  
   [admin-state {enable | disable}]  
   [actor admin-key actor_admin_key]  
   [actor system-priority actor_system_priority]  
   [actor system-id actor_system_id]  
   [partner system-id partner_system_id]  
   [partner system-priority partner_system_priority]  
   [partner admin-key partner_admin_key]  
   [multi-chassis active]  
   [hash {source-mac | destination-mac | source-and-destination-mac | source-ip | destination-ip | source-and-destination-ip | tunnel-protocol}]
```

```
no linkagg lACP agg agg_id[-agg_id2] size size
```

**Syntax Definitions**

- **agg_id[-agg_id2]** The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- **size** The maximum number of links that can belong to the aggregate.
- **name** The name of the dynamic aggregate group. Can be an alphanumeric string. A group name with spaces must be contained within quotes (for example, “Dynamic Group 1”).
- **enable** Specifies that the dynamic aggregate group is active and is able to aggregate links.
- **disable** Specifies that the dynamic aggregate group is inactive and not able to aggregate links.
- **actor_admin_key** The administrative key value associated with the dynamic aggregate group.
- **actor_system_priority** The priority of the dynamic aggregate group.
- **actor_system_id** The MAC address of the dynamic aggregate group on the switch.
- **partner_system_id** The MAC address of the aggregate group of the remote system which is attached to the aggregate group of the switch.
- **partner_system_priority** The priority of the remote system to which the aggregation group is attached.
- **partner_admin_key** The administrative key for the remote partner of the aggregation group.
- **multi-chassis active** This parameter is not supported.
- **source-mac** Selects the source MAC address hashing option.
- **destination-mac** Selects the destination MAC address hashing option.
- **source-and-destination-mac** Selects the source MAC address and destination MAC address hashing option.
source-ip

Selects the source IP hashing option.

destination-ip

Selects the destination IP hashing option.

source-and-destination-ip

Selects the source IP and destination IP hashing option.

tunnel-protocol

Selects the tunnel protocol hashing option.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>hash_option</td>
<td>source-and-destination-ip (Layer 3 traffic)</td>
</tr>
<tr>
<td></td>
<td>source-and-destination-mac (Layer 2 traffic)</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a dynamic aggregate group from the configuration.
- Link aggregation cannot be configured on an AppMon enabled port.
- You must disable the group with the **linkagg lacp agg admin-state** command before you can delete a dynamic link aggregate group.
- Optional parameters for the dynamic aggregate group can be configured when the aggregate is created. The dynamic aggregate group can be modified after the optional parameters are assigned.
- Specify the **hash** parameter option when the link aggregate is first created. The hashing algorithm options apply to unicast traffic and are not modifiable once the aggregate is created. If different options are required:
  - Disassociate all ports currently associated with the aggregate.
  - Delete the aggregate from the switch configuration.
  - Create the aggregate again with the new hashing options.
- It is not necessary to administratively down the linkagg ports before changing the hashing algorithm, but doing so is recommended.
- The hashing algorithm does not take into consideration the speed of the ports to distribute the traffic. In other words, the same number of flows is distributed evenly on each port without consideration of the line speed.
- Aggregate load balancing is performed at the ingress side.
- Per-aggregate hashing is local to the switch, so each side of the aggregation can use different configurations for the hashing algorithms.

- Link aggregation follows the global hash control settings configured through the `hash-control brief` or `hash-control extended` commands.

- For example, if the `source-mac` option is specified for L2 hashing:
  - If the global hash-control is in brief mode, hashing is based on source MAC address only.
  - If the global hash-control is in extended mode, hashing is based on source MAC address, VLAN, Ethertype, and source module ID/port.

- For example, if the `source-ip` option is specified for L3 hashing:
  - If the global hash-control is in brief mode, hashing is based on source IP address only.
  - If the global hash-control is in extended mode, hashing is based on source IP address and source UDP-TCP Port.

- To load balance Unknown Destination/Broadcast/Multicast traffic on all the ports of the aggregate, use the `hash-control` command to enable load balancing of DFL traffic.

- Use the `linkagg static agg size` command to create static aggregate groups. See page 12-3 for more information about this command.

**Examples**

```
-> linkagg lacp agg 2-5 size 4
-> linkagg lacp agg 3 size 2 admin-state disable actor system-priority 65535
-> no linkagg lacp agg 2-5 size 4
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show linkagg` Displays information about static and dynamic (LACP) aggregate groups.

**MIB Objects**

`alclnkaggAggTable`
  - `alclnkaggAggNumber`
  - `alclnkaggAggSize`
  - `alclnkaggAggLacpType`
  - `alclnkaggAggName`
  - `alclnkaggAggAdminState`
  - `alclnkaggAggActorAdminKey`
  - `alclnkaggAggActorSystemPriority`
  - `alclnkaggAggActorSystemID`
  - `alclnkaggAggPartnerSystemID`
  - `alclnkaggAggPartnerSystemPriority`
  - `alclnkaggAggPartnerAdminKey`
  - `alclnkaggAggPortSelectionHash`
linkagg lacp agg name

Configures a name for a dynamic aggregate group.

`linkagg lacp agg agg_id name name`

`no linkagg lacp agg agg_id[agg_id2] name`

**Syntax Definitions**

- `agg_id[agg_id2]`: The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `name`: The name of the dynamic aggregate group. Can be an alphanumeric string. A group name with spaces must be contained within quotes (for example, “Dynamic Group 1”).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a name from a single or a range of dynamic aggregate groups simultaneously.
- Assign names to individual dynamic link aggregate groups separately.

**Examples**

`-> linkagg lacp agg 2 name finance`

`-> no linkagg lacp agg 2-5 name`

**Release History**

Release 7.1.1; command introduced.
Related Commands

- `linkagg lacp agg size` Creates a dynamic aggregate group.
- `show linkagg` Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

- `alclnkaggAggTable`
  - `alclnkaggAggNumber`
  - `alclnkaggAggName`
**linkagg lacp agg wait-to-restore-time**

Configures the number of minutes to wait before bringing up a dynamic link aggregate that is attached to other link aggregates.

```
linkagg lacp agg [agg_id1[-agg_id2]] wait-to-restore-time wtr_minutes

no linkagg lacp agg [agg_id1[-agg_id2]] wait-to-restore-time
```

**Syntax Definitions**

- `agg_id1[-agg_id2]` The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `wtr_minutes` The number of minutes the switch waits to bring a link aggregate up. The range is 0–12 minutes.

**Defaults**

By default, the wait-to-restore timer is set to 0 (disabled).

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the wait-to-restore timer for the specified link aggregate or aggregates.
- If a link aggregate is not attached to other links, this timer value is ignored and the aggregate is immediately brought up.

**Examples**

```
-> linkagg lacp agg 2 wait-to-restore-time 10
-> linkagg lacp agg 2 wait-to-restore-time 0
-> linkagg lacp agg 4 wait-to-restore-time 5
-> no linkagg lacp agg 4 wait-to-restore-time
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **linkagg lacp agg size**: Creates a dynamic aggregate group.
- **show linkagg**: Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

- **alclnkaggAggTable**
  - **alclnkaggAggNumber**
  - **alclnkaggAggWTRTimer**
linkagg lacp agg admin-state

Configures the administrative state of a dynamic aggregate group or a range of dynamic aggregate groups.

linkagg lacp agg agg_id[-agg_id2] admin-state {enable | disable}

**Syntax Definitions**

- `agg_id[-agg_id2]`: The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `enable`: Specifies that the dynamic aggregate group is active and is able to aggregate links.
- `disable`: Specifies that the operation of a dynamic aggregate group cannot be performed.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the administrative state is set to `disable`, the operation of a dynamic aggregation (LACP) group cannot be performed.
- You can also enable or disable the admin-state for a range of link aggregate IDs simultaneously, using this command.

**Examples**

```bash
-> linkagg lacp agg 2 admin-state disable
-> linkagg lacp agg 2-10 admin-state disable
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **linkagg lACP agg size**
  - Creates a dynamic aggregate group.

- **show linkagg**
  - Displays information about static and dynamic (LACP) aggregate groups.

- **show linkagg port**
  - Displays information about ports associated with a particular aggregate group or all aggregates.

MIB Objects

- **alclnkaggAggTable**
  - **alclnkaggAggNumber**
  - **alclnkaggAggAdminState**
**linkagg lACP agg actor admin-key**

Configures the administrative key associated with a dynamic aggregate group.

```
linkagg lACP agg agg_id[agg_id2] actor admin-key actor_admin_key
```

```
no linkagg lACP agg agg_id[agg_id2] actor admin-key
```

### Syntax Definitions

- `agg_id[agg_id2]` The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `actor_admin_key` The administrative key value associated with the dynamic aggregate group.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>actor_admin_key</code></td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `no` form of this command to remove an actor admin key from a dynamic aggregate group.

### Examples

```
-> linkagg lACP agg 3-5 actor admin-key 2
```

```
-> no linkagg lACP agg 3-5 actor admin-key
```

### Release History

Release 7.1.1; command introduced.
Related Commands

**linkagg lacp agg size**
Creates a dynamic aggregate group.

**show linkagg**
Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

alclnkaggAggTable

- alclnkaggAggNumber
- alclnkaggAggActorAdminKey
**linkagg lacp agg actor system-priority**

Configures the priority of the dynamic aggregate group.

```
linkagg lacp agg [agg_id|-agg_id2] actor system-priority actor_system_priority
no linkagg lacp agg [agg_id|-agg_id2] actor system-priority
```

**Syntax Definitions**

- `agg_id|-agg_id2` The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `actor_system_priority` The priority of the dynamic aggregate group of the switch in relation to other aggregate groups.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>actor_system_priority</code></td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to return the value to its default.
- Ports with the same system priority value can join the same dynamic aggregate group.
- To assign or remove the actor system-priority for a series of link aggregate IDs, specify the range of link aggregate IDs with the `agg` keyword. Use a hyphen to separate the first and last link aggregate IDs of a range.

**Examples**

```
-> lacp linkagg 3 actor system-priority 100
-> no lacp linkagg 3 actor system-priority
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **linkagg lACP agg size**
  Creates a dynamic aggregate group.

- **show linkagg**
  Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

- **alclnkaggAggTable**
  - **alclnkaggAggNumber**
  - **alclnkaggAggActorSystemPriority**
linkagg lacp agg actor system-id

Configures the MAC address of a dynamic aggregate group on the switch.

**Syntax**

```
linkagg lacp agg [agg_id][agg_id2] actor system-id actor_system_id
```

**no linkagg lacp agg [agg_id][agg_id2] actor system-id**

**Syntax Definitions**

- `agg_id[agg_id2]` The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>actor_system_id</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the MAC address assignment (actor system ID) from a dynamic link aggregate or a range of dynamic link aggregates simultaneously.

- You can configure the MAC address for a range of dynamic link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range along with this command.

**Examples**

```
-> linkagg lacp agg 2 actor system-id 00:20:da:81:d5:b0
-> no linkagg lacp agg 3-10 actor system-id
-> no linkagg lacp agg 11 actor system-id
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

**linkagg lacp agg size**

Creates a dynamic aggregate group.

**show linkagg**

Displays information about static and dynamic (LACP) aggregate groups.

MIB Objects

alclnkaggAggTable

- **alclnkaggAggNumber**
- **alclnkaggAggActorSystemID**
**linkagg lacp agg partner system-id**

Configures the MAC address of the dynamic aggregate group of the remote system that is attached to the dynamic aggregate group of the local switch.

```plaintext
linkagg lacp agg agg_id[-agg_id2] partner system-id partner_system_id
no linkagg lacp agg agg_id[-agg_id2] partner system-id
```

### Syntax Definitions

- `agg_id[-agg_id2]` The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>partner_system_id</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove a partner system ID from a dynamic aggregate group or a range of groups assigned with the same partner system IDs together.
- The `partner_system_id` and the `partner_system_priority` together specify the priority of the remote system.
- You can configure a partner system ID for a range of dynamic link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range along with this command.

### Examples

- `-> linkagg lacp agg 2 partner system-id 00:20:da4:32:81`
- `-> linkagg lacp agg 2-10 partner system-id 00:20:da4:32:82`
- `-> no linkagg lacp agg 2-10 partner system-id`
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `linkagg lacp agg size`  Creates a dynamic aggregate group.
- `show linkagg`  Displays information about static and dynamic (LACP) aggregate groups.

**MIB Objects**

```
alclnkaggAggTable
   alclnkaggAggNumber
   alclnkaggAggPartnerSystemID
```
linkagg lacp agg partner system-priority

Configures the priority of the dynamic aggregate group of the remote system which is attached to the dynamic aggregate group of the local switch.

```
linkagg lacp agg agg_id[-agg_id2] partner system-priority partner_system_priority

no linkagg lacp agg agg_id[-agg_id2] partner system-priority
```

**Syntax Definitions**

- `agg_id[-agg_id2]` The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `partner_system_priority` The priority of the dynamic aggregate group of the remote system which is attached to the dynamic aggregate group of the local switch.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>partner_system_priority</code></td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32/E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to return to the priority value to its default.
- The `partner_system_id` and the `partner_system_priority` together specify the priority of the remote system.
- You can apply the partner system-priority to a range of link aggregate IDs simultaneously. Use a hyphen to separate the first and last link aggregate IDs of a range after the `agg` keyword.

**Examples**

```
-> linkagg lacp agg 3 partner system-priority 65535
-> linkagg lacp agg 3-6 partner system-priority 65535
-> no linkagg lacp agg 3-6 partner system-priority
```

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- `linkagg lacp agg size`  Creates a dynamic aggregate group.
- `show linkagg`  Displays information about static and dynamic (LACP) aggregate groups.

**MIB Objects**

- `alclnkaggAggTable`
  - `alclnkaggAggNumber`
  - `alclnkaggAggPartnerSystemPriority`
**linkagg lacp agg partner admin-key**

Configures the administrative key for the remote partner of the dynamic aggregation group.

```
linkagg lacp agg agg_id[{-agg_id2}] partner admin-key partner_admin_key
no linkagg lacp agg agg_id[{-agg_id2}] partner admin-key
```

**Syntax Definitions**

- `agg_id[{-agg_id2}]` The link aggregate ID number corresponding to the dynamic aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `partner_admin_key` The administrative key for the remote partner of the dynamic aggregation group.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>partner_admin_key</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a partner admin-key from a dynamic aggregate group.
- The partner admin-key can be assigned for a range of dynamic link aggregate IDs simultaneously.

**Examples**

```
-> linkagg lacp agg 3-5 partner admin-key 3
-> no linkagg lacp agg 3-10 partner admin-key
```

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- `linkagg lACP agg size`  
  Creates a dynamic aggregate group.

- `show linkagg`  
  Displays information about static and dynamic (LACP) aggregate groups.

**MIB Objects**

- `alclnkaggAggTable`  
  - `alclnkaggAggNumber`  
  - `alclnkaggAggPartnerAdminKey`
**linkagg lacp port actor admin-key**

Configures an actor administrative key for a port, which allows the port to join a dynamic aggregate group.

```
linkagg lacp port chassis/slot/port[-port2] actor admin-key actor_admin_key
  [actor admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default]
   [expire] | none}]
  [actor system id actor_system_id]
  [actor system priority actor_system_priority]
  [partner admin system id partner_admin_system_id]
  [partner admin-key partner_admin_key]
  [partner admin system priority partner_admin_system_priority]
  [partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default]
   [expire] | none}]
  [actor port priority actor_port_priority]
  [partner admin port partner_admin_port]
  [partner admin port priority partner_admin_port_priority]
```

```
no linkagg lacp port chassis/slot/port[-port2] [actor admin-state {[active] [timeout] [aggregate]
  [synchronize] [collect] [distribute] [default] [expire] | none}]
  [actor system id actor_system_id]
  [actor system priority actor_system_priority]
  [partner admin system id partner_admin_system_id]
  [partner admin-key partner_admin_key]
  [partner admin system priority partner_admin_system_priority]
  [partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default]
   [expire] | none}]
  [actor port priority actor_port_priority]
  [partner admin port partner_admin_port]
  [partner admin port priority partner_admin_port_priority]
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
- **actor admin-key**: The administrative key associated with this dynamic aggregate group.
- **actor admin-state**: See the linkagg lacp port actor admin-state command.
- **actor system id**: The MAC address of this dynamic aggregate group on the switch.
- **actor system priority**: The priority of the dynamic aggregate group.
- **partner admin system id**: The MAC address of the dynamic aggregate group of the remote switch.
- **partner admin-key**: The administrative key for the remote partner of the dynamic aggregation group.
**Partner admin system priority**  The priority of the remote system to which the dynamic aggregation group is attached.

**Partner admin state**  See the linkagg lacp agg partner admin-state command.

**Actor port priority**  The priority of the actor port.

**Partner admin port**  The administrative state of the partner port.

**Partner admin port priority**  The priority of the partner port.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>active, timeout, aggregate</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to remove a slot and port from a dynamic aggregate group.
- A port can belong to only one aggregate group.
- Ports that belong to a dynamic link aggregate must be configured to the same link speed.
- Ports that belong to the same dynamic aggregate group need not be configured sequentially and can be on any Network Interface (NI).
- Key modification is not allowed without deleting and re-adding the lacp port.

### Examples

- `-> linkagg lacp port 2/1/7 actor admin-key 1`
- `-> no linkagg lacp port 2/1/7`

### Release History

Release 7.1.1; command introduced.

### Related Commands

- **linkagg lacp agg size**  Creates a dynamic aggregate group.
- **show linkagg port**  Displays information about ports associated with a particular aggregate group or all aggregates.
**MIB Objects**

`alclnkaggAggPortTable`

`alclnkaggAggPortGlobalPortNumber`
`alclnkaggAggActorAdminKey`
`alclnkaggAggPortLacpType`
`alclnkaggAggPortActorAdminState`
`alclnkaggAggPortActorSystemID`
`alclnkaggAggPortActorSystemPriority`
`alclnkaggAggPortPartnerAdminSystemID`
`alclnkaggAggPortPartnerAdminKey`
`alclnkaggAggPortPartnerAdminSystemPriority`
`alclnkaggAggPortPartnerAdminState`
`alclnkaggAggPortActorPortPriority`
`alclnkaggAggPortPartnerAdminPort`
`alclnkaggAggPortPartnerAdminPortPriority`
**linkagg lACP port actor admin-state**

Configures the system administrative state of the slot and port for the dynamic aggregate group on the local switch. The state values correspond to bits in the actor state octet in the LACPDU frame.

```
linkagg lACP port chassis/slot/port[-port2] actor admin-state { [active] [timeout] [aggregate]
[synchronize] [collect] [distribute] [default] [expire] | none }
```

```
no linkagg lACP port chassis/slot/port[-port2] actor admin-state { [active] [timeout] [aggregate]
[synchronize] [collect] [distribute] [default] [expire] | none }
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).

- **active**
  - Specifies that bit 0 in the actor state octet is enabled. When this bit is set, the dynamic aggregate group is able to exchange LACPDU frames. By default, this value is set.

- **timeout**
  - Specifies that bit 1 in the actor state octet is enabled. When this bit is set, a short timeout is used for LACPDU frames. When this bit is disabled, a long timeout is used for LACPDU frames. By default, this value is set.

- **aggregate**
  - Specifies that bit 2 in the actor state octet is enabled. When this bit is set, the system considers this port to be a potential candidate for aggregation. If this bit is not enabled, the system considers the port to be individual (it can only operate as a single link). By default, this value is set.

- **synchronize**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 3) is set by the system, the port is allocated to the correct dynamic aggregation group. If this bit is not set by the system, the port is not allocated to the correct dynamic aggregation group.

- **collect**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 4) is set by the system, incoming LACPDU frames are collected from the individual ports that make up the dynamic aggregate group.

- **distribute**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 5) is set by the system, distributing outgoing frames on the port is disabled.

- **default**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 6) is set by the system, it indicates that the actor is using the defaulted partner information administratively configured for the partner.

- **expire**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 7) is set by the system, the actor cannot receive LACPDU frames.

- **none**
  - Resets all administrative states to their default configurations.
### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>[active] [timeout]....</td>
<td>active, timeout, aggregate</td>
</tr>
<tr>
<td>timeout enable</td>
<td>Disabled (OmniSwitch 9900)</td>
</tr>
<tr>
<td></td>
<td>Enabled (All other platforms)</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to restore the LACPDU bit settings to their default configuration.
- When the actor admin-state is set to **none**, all bit values are restored to their default configurations.
- Enabling the **timeout** parameter configures a 1 second interval (short timeout / fast transmit rate). Disabling the **timeout** parameter configures a 30 second interval (long timeout / slow transmit rate).
- **timeout** option when used sets only the transmit rate. The remote side timeout is 3X the configured transmit rate. For example, if the transmit rate is set to 1 packet per second, the remote side will timeout if it misses 3 packets. In this case, it will timeout in 3 seconds. If the transmit rate is set to 30 packets per second, then the remote side will take 90 seconds to timeout.
- ‘no linkagg lacp port actor admin-state timeout’ disables the **timeout** parameter, which results in a long timeout, that is, 30 second transmission rate.

### Examples

```
-> linkagg lacp port 4/2 actor admin-state synchronize collect distribute
-> no linkagg lacp port 4/2 actor admin-state synchronize collect
-> linkagg lacp port 4/2 actor admin-state none
```

### Release History

Release 7.1.1; command introduced.
Related Commands

- **linkagg lacp agg size**  
  Creates a dynamic aggregate group.

- **show linkagg port**  
  Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

- **alclnkaggAggPortTable**
- **alclnkaggAggPortGlobalPortNumber**
- **alclnkaggAggPortActorAdminState**
linkagg lacp port actor system-id

Configures the system ID (i.e., MAC address) for the local port associated with a dynamic aggregate group.

linkagg lacp port chassis/slot/port[-port2] actor system-id actor_system_id

no linkagg lacp port chassis/slot/port[-port2] actor system-id

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>actor_system_id</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the no form of this command to remove the actor system ID from a slot and port or a range of slot and ports associated with a dynamic aggregate group.
- Configure the system ID for a range of local ports simultaneously. Use a hyphen to separate the first and last port IDs of a range after the port keyword.

**Examples**

- `-> linkagg lacp port 3/1-10 actor system-id 00:20:da:06:ba:d3`
- `-> no linkagg lacp port 3/1-10 actor system-id`

**Release History**

Release 7.1.1; command introduced.
Related Commands

`linkagg lacp agg size`  Creates a dynamic aggregate group.
`show linkagg port`  Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

`alclnkaggAggPortTable`
  `alclnkaggAggPortGlobalPortNumber`
  `alclnkaggAggPortActorSystemID`
linkagg lacp port actor system-priority

Configures the system priority of the port on the switch that belongs to the dynamic aggregate group.

**linkagg lacp port** *chassis/slot/port[-port2] actor system-priority actor_system_priority*

**no linkagg lacp port** *chassis/slot/port[-port2] actor system-priority*

### Syntax Definitions

- **chassis** The chassis identifier.
- **slot/port[-port2]** The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
- **actor_system_priority** The priority of the dynamic aggregate group.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>actor_system_priority</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove an actor system priority value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

- Configure the actor system-priority to a range of ports simultaneously. Use a hyphen to separate the first and last port of a range after the **port** keyword.

### Examples

```
-> linkagg lacp port 3/2-10 actor system-priority 65
-> no linkagg lacp port 3/2-10 actor system-priority
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- `linkagg lacp agg size`  Creates a dynamic aggregate group.
- `show linkagg port`  Displays information about ports associated with a particular aggregate group or all aggregates.

**MIB Objects**

- `AlcLnkAggAggPortTable`
  - `alclnkaggAggPortGlobalPortNumber`
  - `alclnkaggAggPortActorSystemPriority`
**linkagg lacp agg partner admin-state**

Configures the system administrative state of the slot and port for the dynamic aggregate group on the remote switch. The state values correspond to bits in the actor state octet in the LACPDU frame.

```
linkagg lacp port chassis/slot/port[-port2] partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}
```

```
no linkagg lacp port chassis/slot/port[-port2] partner admin-state {[active] [timeout] [aggregate] [synchronize] [collect] [distribute] [default] [expire] | none}
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).

- **active**
  - Specifies that bit 0 in the partner state octet is enabled. When this bit is set, the dynamic aggregate group is able to exchange LACPDU frames. By default, this value is set.

- **timeout**
  - Specifies that bit 1 in the partner state octet is enabled. When this bit is set, a short timeout is used for LACPDU frames. When this bit is disabled, a long timeout is used for LACPDU frames. By default, this value is set.

- **aggregate**
  - Specifies that bit 2 in the partner state octet is enabled. When this bit is set, the system considers this port to be a potential candidate for aggregation. If this bit is not enabled, the system considers the port to be individual (it can only operate as a single link). By default, this value is set.

- **synchronize**
  - Specifies that bit 3 in the partner state octet is enabled. When this bit is set, the port is allocated to the correct dynamic aggregation group. If this bit is not enabled, the port is not allocated to the correct aggregation group. By default, this value is disabled.

- **collect**
  - Specifying this keyword has no effect because the system always determines its value. When this bit (bit 4) is set by the system, incoming LACPDU frames are collected from the individual ports that make up the dynamic aggregate group.

- **distribute**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 5) is set by the system, distributing outgoing frames on the port is disabled.

- **default**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 6) is set by the system, it indicates that the partner is using the defaulted actor information administratively configured for the actor.

- **expire**
  - Specifying that this keyword has no effect because the system always determines its value. When this bit (bit 7) is set by the system, the partner cannot receive LACPDU frames.

- **none**
  - Resets all administrative states to their default configurations.
**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>[active] [timeout]</td>
<td>active, timeout, aggregate</td>
</tr>
<tr>
<td>timeout enable</td>
<td>Disabled (OmniSwitch 9900)</td>
</tr>
<tr>
<td></td>
<td>Enabled (All other platforms)</td>
</tr>
<tr>
<td>timeout enable</td>
<td>Disabled (OmniSwitch 9900)</td>
</tr>
<tr>
<td></td>
<td>Enabled (All other platforms)</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to restore the LACPDU bit settings to their default configuration for a single port or a range of ports.

- When the partner admin-state is set to **none**, all bit values are restored to their default configurations.

- Configure the system administrative state for a range of ports simultaneously. Use a hyphen to separate the first and last port of a range after the **port** keyword.

- Enabling the **timeout** parameter configures a 1 second interval (short timeout / fast transmit rate). Disabling the **timeout** parameter configures a 30 second interval (long timeout / slow transmit rate).

- **timeout** option when used sets only the transmit rate. The remote side timeout is 3X the configured transmit rate. For example, if the transmit rate is set to 1 packet per second, the remote side will timeout if it misses 3 packets. In this case, it will timeout in 3 seconds. If the transmit rate is set to 30 packets per second, then the remote side will take 90 seconds to timeout.

- ‘no linkagg lacp port partner admin-state’ disables the **timeout** parameter, which results in a long timeout, that is, 30 second transmission rate.

**Examples**

- `-> lacp port 4/2-10 partner admin-state synchronize collect distribute`
- `-> no lacp agg 4/2-10 partner admin-state synchronize collect`

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- `linkagg lacp agg size`  Creates a dynamic aggregate group.
- `show linkagg port`  Displays information about ports associated with a particular aggregate group or all aggregate groups.

**MIB Objects**

- `alclnkaggAggPortTable`
- `alclnkaggAggPortGlobalPortNumber`
- `alclnkaggAggPortPartnerAdminState`
**linkagg lACP port partner admin system-id**

Configures the partner administrative system ID for a dynamic aggregate group port.

```
linkagg lACP port chassis/slot/port[-port2] partner admin system-id partner_admin_system_id
no linkagg lACP port chassis/slot/port[-port2] partner admin system-id
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).

- **partner_admin_system_id**

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>partner_admin_system_id</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `no` form of this command to remove a partner administrative system ID from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

### Examples

```
-> linkagg lACP port 3/1-10 partner admin system-id 00:20:da:05:f6:23
```

### Release History

Release 7.1.1; command introduced.
Related Commands

- `linkagg lacp agg size` Creates a dynamic aggregate group.
- `show linkagg port` Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

- `AlcLnkAggAggPortTable`
- `alclnkaggAggPortGlobalPortNumber`
- `alclnkaggAggPortPartnerAdminSystemID`
**linkagg lacp port partner admin-key**

Configures the partner administrative key for a dynamic aggregate group port.

```
linkagg lacp port chassis/slot/port[-port2] partner admin-key partner_admin_key
no linkagg lacp port chassis/slot/port[-port2] partner admin-key
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).

- **partner_admin_key**
  - The administrative key for the remote partner of a dynamic aggregation group.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>partner_admin_key</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a partner admin key value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

- Key modification is not allowed without deleting and re-adding the lacp port.

**Examples**

```
--> linkagg lacp port 1/2/1-5 partner admin-key 1
--> no linkagg lacp port 1/2/1-5
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

**linkagg lacp agg size**  Creates a dynamic aggregate group.

**show linkagg port**  Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

AlcLnkAggAggPortTable

- alclnkaggAggPortGlobalPortNumber
- alclnkaggAggPortPartnerAdminKey
**linkagg lACP port partner admin system-priority**

Configures the partner system priority for a dynamic aggregate group port.

```
linkagg lACP port chassis/slot/port[-port2] partner admin system-priority

no linkagg lACP port chassis/slot/port[-port2] partner admin system-priority
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
- **partner_admin_system_priority**: The priority of the dynamic aggregate group of the remote switch to which the aggregation group is attached.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>partner_admin_system_priority</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to remove a `partner_system_priority` value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

**Examples**

```
-> linkagg lACP port 2/1-5 partner admin system-priority 65
-> no linkagg lACP port 2/1-5 partner admin system-priority
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- `linkagg lacp agg size`  Creates a dynamic aggregate group.
- `show linkagg port`  Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

- `AlcLnkAggAggPortTable`
  - `alclnkaggAggPortGlobalPortNumber`
  - `alclnkaggAggPortAdminSystemPriority`
**linkagg lacp port actor port priority**

Configures the priority for an actor port.

```
linkagg lacp port chassis/slot/port[-port2] actor port-priority actor_port_priority
no linkagg lacp port chassis/slot/port[-port2] actor port-priority
```

**Syntax Definitions**

- `chassis`  
  The chassis identifier.

- `slot/port[-port2]`  
  The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).

- `actor_port_priority`  
  The priority of the actor port.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>actor_port_priority</code></td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to remove an `actor_port_priority` value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

**Examples**

```
-> linkagg lacp port 2/1-5 actor port-priority 100
-> no linkagg lacp port 2/1-5 actor port-priority
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- `linkagg lACP agg size` Creates a dynamic aggregate group.
- `show linkagg port` Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

AlcLnkAggAggPortTable
- `alclnkaggAggPortGlobalPortNumber`
- `alclnkaggAggPortActorPortPriority`
**linkagg lACP port partner admin-port**

Configures the administrative status of a partner port.

```
linkagg lACP port chassis/slot/port[-port2] partner admin-port partner_admin_port
no linkagg lACP port chassis/slot/port[-port2] partner admin-port
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
- `partner_admin_port` The administrative state of the partner port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8</th>
<th>C32E/T24C2</th>
<th>9900</th>
<th>9900X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to remove a `partner_admin_port` value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

**Examples**

- `-> linkagg lACP port 2/1-5 partner admin-port 255`
- `-> no linkagg lACP port 2/1-5 partner admin-port`

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **linkagg lacp agg size**
  Creates a dynamic aggregate group.

- **show linkagg port**
  Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

- **AlcLnkAggAggPortTable**
  - **alclnkaggAggPortGlobalPortNumber**
  - **alclnkaggAggPortPartnerAdminPort**
**linkagg lacp port partner admin port-priority**

Configures the priority for a partner port.

```
linkagg lacp port chassis/slot/port[-port2] partner admin port-priority partner_admin_port_priority
no linkagg lacp port chassis/slot/port[-port2] partner admin port-priority
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot number for this aggregate and the port that the switch initially uses as the Spanning Tree virtual port for this aggregate. Use a hyphen to specify a range of ports (2/1-5).
- `partner_admin_port_priority` The priority of the partner port.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>partner_admin_port_priority</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to remove a `partner_admin_port_priority` value from a slot and port or a range of slot and ports associated with a dynamic aggregate group.

**Examples**

```
-> linkagg lacp port 2/1-5 partner admin port-priority 100
-> no linkagg lacp port 2/1-5 partner admin port-priority
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **linkagg lacp agg size**  
  Creates a dynamic aggregate group.

- **show linkagg port**  
  Displays information about ports associated with a particular aggregate group or all aggregate groups.

MIB Objects

- **AlcLnkAggAggPortTable**
  - **alcLnkaggAggPortGlobalPortNumber**
  - **alcLnkaggAggPortPartnerAdminPortPriority**
**dhl name**

Configures a Dual-homed Link (DHL) session associated with the specified session ID number.

`dhl dhl_num [name name]`

`no dhl dhl_num`

---

**Syntax Definitions**

- `dhl_num` The DHL session ID number. Valid range is 1–1000.
- `name` The name of the DHL session.

**Defaults**

By default, if a name is not assigned to a DHL session, the session is configured as DHL-1.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6450</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a DHL session ID from the switch configuration.
- Use the optional `name` parameter to specify a name for the DHL session.
- Only one DHL session can be configured on a switch.
- Once the DHL session ID is created, assign a link A port and a link B port to the session. This is required before administratively enabling the DHL session is allowed.

**Examples**

- `dhl 1 name dhl_session1`
- `no dhl 1`

**Release History**

Release 8.2.1; command was introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhl linka linkb</td>
<td>Associates a pair of links (port or linkagg) with the DHL session.</td>
</tr>
<tr>
<td>dhl admin-state</td>
<td>Configures the administrative status of the DHL session.</td>
</tr>
<tr>
<td>show dhl</td>
<td>Displays information about a specific DHL session.</td>
</tr>
</tbody>
</table>

### MIB Objects

- `alaDHLSessionTable`
  - `alaDHLSessionIndex`
  - `alaDHLSessionDescr`
**dhl linka linkb**

Configures two ports or two link aggregates or a combination of both as linkA and linkB for the specified DHL session. Only two links are allowed per DHL session; only one DHL session per switch is allowed.

```
dhl num linka {port chassis/slot/port | linkagg agg_id} linkb {port chassis/slot/port | linkagg agg_id}
```

```
no dhl num linka {port chassis/slot/port | linkagg agg_id} linkb {port chassis/slot/port | linkagg agg_id}
```

**Syntax Definitions**

- **dhl_num**: An existing DHL session ID number.
- **chassis**: The chassis ID number.
- **slot**: The slot number to designate as a link for the DHL session.
- **port**: The physical port number to designate as a link for the DHL session.
- **agg_id**: The link aggregate ID number to designate as a link for the DHL session.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the linkA and linkB ports from the specified session ID. Before attempting to remove the links, administratively disable the DHL session.
- Make sure that DHL linkA and linkB are associated with each of the VLAN that the DHL session will protect. Any VLAN not associated with both the links or only associated with one of the links is unprotected.
- DHL linkA and linkB should belong to the same default VLAN. In addition, select a default VLAN that is one of the VLANs that the DHL session will protect. For example, if the session is going to protect VLANs 10-20, then assign one of those VLANs as the default VLAN for linkA and linkB.
- Only one DHL session per switch is allowed. Each session can have only two links (linkA and linkB). Specify a physical switch port or a link aggregate (linkagg) ID as a DHL link. The same port or link aggregate is not configurable as both linkA or linkB.
- DHL is not supported on mobile, 802.1x-enabled, GVRP, or UNI ports. DHL is also not supported on a port that is a member of a link aggregate or a port that is enabled for transparent bridging.

- The administrative state of a DHL session is not configurable until a linkA port and a linkB port are associated with the specified DHL session ID number.

- Changing the port designations for linkA and linkB is not recommended while the DHL session is enabled.

- Removing a link aggregate from the switch configuration is not allowed if the aggregate is configured as a link for a DHL session.

**Examples**

- `dhl 1 linka port 1/1 linkb port 1/2`
- `dhl 1 linka  linkagg 1  linkb port 1/2`
- `dhl 1 linka port 1/1 linkb linkagg 1`
- `dhl 1 linka  linkagg 1  linkb linkagg 2`
- `no dhl 1 linka port 1/1 linkb port 1/2`

**Release History**

Release 8.2.1; command was introduced.

**Related Commands**

- `dhl name` Configures a session ID for the DHL session.
- `dhl admin-state` Configures the administrative status for the DHL session.
- `show dhl` Displays the global status of the DHL configuration.
- `show dhl` Displays information about a specific DHL session.
- `show dhl link` Displays information about a specific link.

**MIB Objects**

- `AlaDHLLinksTable`
  - `alaDHLLinksSessionIndex`
  - `alaDHLLinkslinkA`
  - `alaDHLLinkslinkB`
**dhl admin-state**

Enables or disables the administrative state of a DHL session.

```
dhl dhl_num admin-state {enable | disable}
```

---

### Syntax Definitions

- **dhl_num**: An existing DHL session ID number.
- **enable**: Enables the DHL session.
- **disable**: Disables the DHL session.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- The DHL session ID specified with this command must already exist in the switch configuration.
- The administrative state cannot be enabled until a linkA port and a linkB port are associated with the specified DHL session ID number.

---

### Examples

```
-> dhl 1 admin-state enable
-> dhl 1 admin-state disable
```

---

### Release History

Release 8.2.1; command was introduced.
Related Commands

**dhl name**
Configures a session ID for the DHL session.

**dhl admin-state**
Configures the administrative status for the DHL session.

**show dhl**
Displays the global status of the DHL configuration or information about a specific DHL session.

MIB Objects

alaDHLSessionTable

alaDHLSessionAdminStatus
**dhl vlan-map linkb**

Configures a VLAN-MAP (a single VLAN or a range of VLANs) from a common pool of VLANs to operate on DHL link B.

```
dhl dhl_num vlan-map linkb {vlan_id[-vlan_id]}
no dhl dhl_num vlan-map linkb {vlan_id[-vlan_id]}
```

**Syntax Definitions**

- **dhl_num**
  - A DHL session ID number.

- **vlan_id[-vlan_id]**
  - A VLAN ID number or a range of VLAN IDs to map to linkB. The valid range is 1–4094.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A DHL session has to be created before a VLAN-MAP can be configured.

- When the DHL session is active, the common VLAN that both the dual homed links belong to is treated as a protected VLAN. The VLAN containing only one dual homed link is treated as an unprotected VLAN. Traffic is forwarded only on the dual homed links belonging to the protected VLAN.

- If a VLAN is removed globally and if the VLAN belongs to a particular dual homed link, then the VLAN will automatically be removed from the dual homed link.

- If one dual homed link, for example linkA, is moved out of a protected VLAN, then the VLAN becomes unprotected and the VPA is removed from the second dual homed link, for example linkB.

- If the admin state of a VLAN is changed to disabled, and if the VLAN is part of a protected VLAN, then the disabled VLAN is removed from the operational DHL VLAN list but will be present in the protected VLAN list.

- If the admin state of a dual homed link, for example linkA, is changed to disabled, then the protected VLANs of the disabled linkA are moved to the other link, for example linkB. When linkA is re-enabled, then the VLANs are moved back to linkA.
If the VLAN-MAP of linkB is removed, then the VPAs for the linkB will also be removed and the VLANs configured on linkB are moved to linkA.

If a VLAN is configured as default on one dual homed link, for example linkA, then the same VLAN cannot be configured as tagged on the other link, for example linkB.

Examples

```
-> vlan 10-30
-> vlan 10-20 802.1q 1/1
-> vlan 4
-> vlan port default 1/1-2
-> dhl 1 name dhl_session1
-> dhl 1 linka port 1/1 linkb port 1/2
-> dhl 1 vlan-map linkb 18-20
-> no dhl 1 vlan-map linkb 18-20
```

Release History

Release 8.2.1; command was introduced.

Related Commands

- `dhl name` Configures a session ID for the DHL session.
- `dhl admin-state` Configures the administrative status for the DHL session.
- `show dhl` Displays the global status of the DHL configuration or information about a specific DHL session.
- `show dhl link` Displays information about a specific link.

MIB Objects

- `alaDHLVlanMapTable`
  - `alaDHLVlanMapSessionIndex`
  - `alaDHLVlanMapVlanStart`
  - `alaDHLVlanMapVlanEnd`
  - `alaDHLVlanMapRowStatus`
**dhl pre-emption-time**

Configures the pre-emption timer for the DHL session. A pre-emption timer is a recovery-delay timer that is used to delay the switchover of VLANs to their primary links. It is the delay in the resumption of traffic when a link that is down is brought up.

**dhl dhl_num pre-emption-time seconds**

---

**Syntax Definitions**

* dhl_num
  A DHL session ID number.

* seconds
  The number of seconds for the delay in the switchover of VLANs to their primary links. The valid range is 0–600.

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>30 seconds</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Pre-emption timer is applicable only when a failed port is brought up. If both ports are down, the pre-emption timer is activated only when the second port is brought up.

- If the pre-emption timer value is set to 0, then there will be no delay in the VLANs being moved back to their primary link.

- If a link fails when the pre-emption timer is active, that is when the remaining pre-emption time value is not equal to 0, then the timer will be halted.

- When the pre-emption timer is active for a particular link and if the other link goes down, then the VLANs of the link that is down are automatically moved to the port for which the pre-emption timer is active.

- When DHL ports spanned across the NIs or DHC ports are on the same NI but data port is on different NI, it is advised to configure mac-flush mechanism (either Raw/MVRP) for faster convergence.

---

**Examples**

-> dhl 1 pre-emption-time 40sec
Release History

Release 8.2.1; command was introduced.

Related Commands

- **dhl name**: Configures a session ID for the DHL session.
- **show dhl**: Displays the global status of the DHL configuration or information about a specific DHL session.
- **show dhl link**: Displays information about a specific link.

MIB Objects

- **alaDHLSessionTable**
  - **alaDHLSessionPreemptionTime**
dhl mac-flushing

Configures the MAC-flushing technique for the DHL session. The MAC-flushing technique is used to correct any stale MAC entries that are caused when a dual homed link goes down.

```
dhl dhl_num mac-flushing {none | raw | mvrp}
```

**Syntax Definitions**

- **dhl_num**  
  A DHL session ID number.

- **none**  
  Flushing of the MAC address tables does not occur.

- **raw**  
  Method of flushing when VPAs of the links moved across them due to link up/down or configuration change (VLAN-map). The switch determines the MAC addresses within the affected VLANs.

- **mvrp**  
  Method of flushing when one link fails and the other link issues 'join' declarations to establish connectivity. These new joins are flagged as 'new' and they are forwarded by the core devices causing flushing on the core network for the active VLANs.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>raw</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Before enabling MVRP on dual homed links, the Registrar Mode should be set to 'forbidden', failing which an error message is displayed when configuring DHL. If the Registrar Mode is set to 'not forbidden', then changes cannot be made to the MVRP configuration on the dual homed links.

- If the MAC-flushing technique is set to MVRP and if MVRP is not enabled on the dual homed links, then the `show dhl` command displays the active MAC-flushing technique as **none**. When MVRP is enabled on the dual homed links, then the MAC-flushing technique changes to **MVRP** and the Registrar Mode of the links is automatically set to ‘forbidden’.

- If VLANs are moved across the dual homed links as a result of configuration changes, then MAC-flushing is automatically enabled, if configured, excepting dual homed links that are changed on the fly.
**Examples**

-> dhl 1 mac-flushing none  
-> dhl 1 mac-flushing raw

**Release History**

Release 8.2.1; command was introduced.

**Related Commands**

- **dhl name**
  Configures a session ID for the DHL session.

- **show dhl**
  Displays the global status of the DHL configuration or information about a specific DHL session.

- **show dhl link**
  Displays information about a specific link.

**MIB Objects**

alaDHLSessionTable  
  alaDHLSessionMacFlushingtech
**show dhl**

Displays the global status of the DHL configuration or information about a specific DHL session.

`show dhl [dhl_num]`

### Syntax Definitions

- **dhl_num**: A DHL session ID number.

### Defaults

By default, the global status of the DHL configuration is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `dhl_num` parameter to display information about a specific DHL session.

### Examples

```
-> show DHL
Number Name Admin state Oper state Pre-emption time Mac-flushing Active Mac-flushing
------------------------------+--------------------------+-------------------------------+--------------------------
  1  DHL-1   UP    UP  30sec     Raw          Raw
```

**output definitions**

- **Number**: Number of the DHL session.
- **Name**: The user-defined text description of the DHL session.
- **Admin state**: The administrative status of the DHL session.
- **Oper state**: The operational status of the DHL session.
- **Pre-emption time**: The pre-emption time in seconds of the DHL session.
- **Mac-flushing**: Mac-flushing technique on the DHL session.
- **Active Mac-flushing**: Mac-flushing technique that is currently active on the DHL session.

```
-> show dhl 1
DHL session name : Arice,
Admin state     : Up,
Operational state: Up,
```
Pre-emption time : 40 sec,
Mac-flushing : Raw-Flushing,
Active Mac-flushing : Raw-Flushing,

Protected VLANs : 10-20,23,25,30-100,600,700,800,

linkA:
  Port : 1/2,
  Operational state : Up

  Un protected VLANs : 900,1980,1987,234,
  Active VLAN : 10-20,23,25,30-100,600,700,800,

linkB:
  Port : 1/1,
  Operational state : Down,
  Un protected VLANs : 1730-1800,
  Vlan-map : 30-100,600,
  Active Vlans : none,

output definitions

<table>
<thead>
<tr>
<th>DHL session Name</th>
<th>The user-defined text description of the DHL session.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin state</td>
<td>The current administrative status of the DHL session.</td>
</tr>
<tr>
<td>Operational state</td>
<td>The operational state of the DHL session.</td>
</tr>
<tr>
<td>Pre-emption time</td>
<td>The delay-interval in seconds to move the VLANs back to their original links.</td>
</tr>
<tr>
<td>Mac-flushing</td>
<td>Mac-flushing technique on the DHL session.</td>
</tr>
<tr>
<td>Active Mac-flushing</td>
<td>The active Mac-flushing technique that is enabled on the specified DHL session.</td>
</tr>
<tr>
<td>Protected VLANs</td>
<td>The common VLANs that contain both the dual homed links, for example linkA and linkB.</td>
</tr>
<tr>
<td>LinkA</td>
<td>A dual homed link that is part of a pair of DHL links that can be configured per switch.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number of linkA.</td>
</tr>
<tr>
<td>Operational state</td>
<td>The operational state of the port. The operational states are UP or DOWN.</td>
</tr>
<tr>
<td>Un protected VLANs</td>
<td>The VLANs containing only one dual homed link.</td>
</tr>
<tr>
<td>Active VLANs</td>
<td>The VLANs that are in an active state.</td>
</tr>
<tr>
<td>LinkB</td>
<td>A dual homed link that is part of a pair of DHL links that can be configured per switch.</td>
</tr>
<tr>
<td>Port</td>
<td>The port number of linkB.</td>
</tr>
<tr>
<td>Operational state</td>
<td>The operational state of the port. The operational states are UP or DOWN.</td>
</tr>
<tr>
<td>Un protected VLANs</td>
<td>The VLANs containing only one dual homed link.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.2.1; command was introduced.

**Related Commands**

- **dhl name** Configures a session ID for the DHL session.
- **show dhl link** Displays information about a specific link.

**MIB Objects**

alaDHLSessionTable
  - alaDHLSessionIndex
  - alaDHLSessionDesc
  - alaDHLSessionAdminStatus
  - alaDHLSessionOperStatus
  - alaDHLSessionPreemptionTime
  - alaDHLSessionMacFlushingtech

alaDHLLinksTable
  - alaDHLLinksSessionIndex
  - alaDHLLinkslinkA
  - alaDHLLinkslinkAOperStatus
  - alaDHLLinkslinkB
  - alaDHLLinkslinkBOperStatus

alaDHLVlanMapTable
  - alaDHLVlanMapSessionIndex
  - alaDHLVlanMapVlanStart
  - alaDHLVlanMapVlanEnd

alaDHLVpaTable
  - alaDHLVpalink
  - alaDHLVpaVlan
  - alaDHLVpaVlanType
  - alaDHLVpaOperationalLink

---

**output definitions**

<table>
<thead>
<tr>
<th>VLAN-map</th>
<th>The DHL VLAN map for linkB. This specifies the VLANs that are operational on DHL linkB from the common pool of VLANs between DHL linkA and linkB.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational VLANs</td>
<td>The VLANs that are in an operational state.</td>
</tr>
</tbody>
</table>
show dhl link

Displays information about a specific DHL link, for example linkA or linkB and the VLAN details of the specified link.

show dhl dhl_num [linkA | linkB]

---

**Syntax Definitions**

dhl_num

A DHL session ID number.

linkA

The dual homed link that is part of a pair of DHL links that can be configured per switch.

linkB

The dual homed link that is part of a pair of DHL links that can be configured per switch.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

-> show dhl 1 linkA

linkA:

<table>
<thead>
<tr>
<th>Port</th>
<th>Operational state</th>
<th>Protected VLANs</th>
<th>Un protected VLANs</th>
<th>Active VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2</td>
<td>Up</td>
<td>10-20, 23, 25, 30-100, 600, 700, 800</td>
<td>900, 1980, 1987, 234</td>
<td>10-20, 23, 25, 30-100, 600, 700, 800</td>
</tr>
</tbody>
</table>

---

**Release History**

Release 8.2.1; command was introduced.
Related Commands

**dhl name**
Configures a session ID for the DHL session.

**dhl linka linkb**
Configures a port or a link aggregate as dual homed links (linkA, linkB) of a DHL session.

**dhl vlan-map linkb**
Configures a VLAN or a range of VLANs from a common pool to operate on DHL linkB.

**show dhl**
Displays information about a specific DHL session.

MIB Objects

**alaDHLLinksTable**
- alaDHLLinksSessionIndex
- alaDHLLinkslinkA
- alaDHLLinkslinkAOperStatus
- alaDHLLinkslinkkB

**alaDHLVpaTable**
- alaDHLVpalink
- alaDHLVpaVlan
- alaDHLVpaVlanType
- alaDHLVpaOperationalLink

**alaDHLVlanMapTable**
- alaDHLVlanMapSessionIndex
- alaDHLVlanMapVlanStartala
- alaDHLVlanMapVlanEnd
show linkagg

Displays information about static and dynamic (LACP) aggregate groups.

show linkagg [agg agg_id1[-agg_id2]]

Syntax Definitions

agg_id1[-agg_id2] The link aggregate ID number corresponding to the aggregate group. Configured through the linkagg static agg size or linkagg lacp agg size command. Use a hyphen to specify a range of IDs (10-20).

Defaults

By default, information for all aggregate groups is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If an aggregate number is specified, only the information about the relevant aggregate group is displayed. The fields included in the display depend on whether the aggregate group is static or dynamic.

- Use the show linkagg port command to display information about aggregate group ports.

Examples

No aggregate group is specified:

-> show linkagg

<table>
<thead>
<tr>
<th>Number</th>
<th>Aggregate</th>
<th>SNMP Id</th>
<th>Size</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Att/Sel Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Static</td>
<td>40000001</td>
<td>8</td>
<td>ENABLED</td>
<td>UP</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Dynamic</td>
<td>40000002</td>
<td>4</td>
<td>ENABLED</td>
<td>DOWN</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Dynamic</td>
<td>40000003</td>
<td>8</td>
<td>ENABLED</td>
<td>DOWN</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Dynamic</td>
<td>40000004</td>
<td>8</td>
<td>ENABLED</td>
<td>UP</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Static</td>
<td>40000005</td>
<td>2</td>
<td>DISABLED</td>
<td>DOWN</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>Loopback</td>
<td>40000010</td>
<td>2</td>
<td>ENABLED</td>
<td>DOWN</td>
<td>0</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Number</th>
<th>The aggregate group number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate</td>
<td>The type of aggregate group (Static, Dynamic, or Loopback).</td>
</tr>
</tbody>
</table>
A static aggregate is specified:

-> show linkagg agg 5

Static Aggregate

  SNMP Id                   : 40000005,
  Aggregate Number          : 5,
  SNMP Descriptor           : Omnichannel Aggregate Number 5 ref 40000005 size 2,
  Name                      : AGG5,
  Admin State               : ENABLED,
  Operational State         : DOWN,
  Aggregate Size            : 2,
  Number of Selected Ports  : 0,
  Number of Reserved Ports  : 0,
  Number of Attached Ports  : 0,
  Primary Port              : NONE
  Port Selection Hash       : Source Destination Ip,
  Wait To Restore Time      : 0 Minutes

-> show linkagg agg 10

Static Loopback Aggregate

  SNMP Id                   : 40000010,
  Aggregate Number          : 20,
  SNMP Descriptor           : Omnichannel Aggregate Number 20 ref 40000020 size 2,
  Name                      : AGG5,
  Admin State               : ENABLED,
  Operational State         : DOWN,
  Aggregate Size            : 2,
  Number of Selected Ports  : 0,
  Number of Reserved Ports  : 0,
  Number of Attached Ports  : 0,
  Primary Port              : NONE
  Port Selection Hash       : Source Destination Ip,
  Wait To Restore Time      : 0 Minutes

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Id</td>
<td>The SNMP ID associated with the aggregate group.</td>
</tr>
<tr>
<td>Size</td>
<td>The number of links in this aggregate group.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The current administrative state of the aggregate group (ENABLED or DISABLED). Configured through the linkagg static agg admin-state command for static aggregate groups and the linkagg lacp agg admin-state command for dynamic aggregate groups.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The current operational state of the aggregate group (UP or DOWN).</td>
</tr>
<tr>
<td>Att Ports</td>
<td>The number of ports actually attached to this aggregate group.</td>
</tr>
<tr>
<td>Sel Ports</td>
<td>The number of ports that could possibly attach to the aggregate group.</td>
</tr>
</tbody>
</table>

output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Id</td>
<td>The SNMP ID associated with this static aggregate group.</td>
</tr>
<tr>
<td>Aggregate Number</td>
<td>The group number.</td>
</tr>
<tr>
<td>SNMP Descriptor</td>
<td>The standard MIB name for this static aggregate group.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of this static aggregate group. Configured through the linkagg static agg name command.</td>
</tr>
</tbody>
</table>
A dynamic aggregate group is specified:

`-> show linkagg agg 1-2`

Dynamic Aggregate
- SNMP Id: 40000002,
- Aggregate Number: 2,
- SNMP Descriptor: Dynamic Aggregate Number 2 ref 40000002 size 4,
- Name: AGG 2,
- Admin State: ENABLED,
- Operational State: DOWN,
- Aggregate Size: 4,
- Number of Selected Ports: 0,
- Number of Reserved Ports: 0,
- Number of Attached Ports: 0,
- Primary Port: NONE,
- Port Selection Hash: Source Destination Ip,
- Wait To Restore Time: 0 Minutes

LACP
- MACAddress: [00:1f:cc:00:00:00],
- Actor System Id: [00:20:da:81:d5:b0],
- Actor System Priority: 50,
- Actor Admin Key: 120,
- Actor Oper Key: 0,
- Partner System Id: [00:20:da:81:d5:b1],
- Partner System Priority: 70,
- Partner Admin Key: 220,
- Partner Oper Key: 0

output definitions (continued)

<table>
<thead>
<tr>
<th>Admin State</th>
<th>The administrative state of this static aggregate group (ENABLED or DISABLED). Configured through the <code>linkagg static agg admin-state</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational State</td>
<td>The operational state of this static aggregate group (UP or DOWN).</td>
</tr>
<tr>
<td>Aggregate Size</td>
<td>The number of links configured for this static aggregate group.</td>
</tr>
<tr>
<td>Number of Selected Ports</td>
<td>The number of ports that could possibly attach to this static aggregate group.</td>
</tr>
<tr>
<td>Number of Reserved Ports</td>
<td>The total number of ports reserved for use in link aggregation by this static aggregate group. (Note: This field is not relevant for static aggregate groups.)</td>
</tr>
<tr>
<td>Number of Attached Ports</td>
<td>The number of ports actually attached to this static aggregate group.</td>
</tr>
<tr>
<td>Primary Port</td>
<td>The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.</td>
</tr>
<tr>
<td>Port Selection Hash</td>
<td>The hashing algorithm used to identify a specific traffic flow to hash.</td>
</tr>
<tr>
<td>Wait To Restore Time</td>
<td>The amount of time, in minutes, the switch waits to bring up a link aggregate that is attached to other links. Configured through the <code>linkagg static agg wait-to-restore-time</code> command.</td>
</tr>
</tbody>
</table>
### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Id</td>
<td>The SNMP ID associated with this dynamic aggregate group.</td>
</tr>
<tr>
<td>Aggregate Number</td>
<td>The group number of this dynamic aggregate group.</td>
</tr>
<tr>
<td>SNMP Descriptor</td>
<td>The standard MIB name for this dynamic aggregate group.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of this dynamic aggregate group. Configured through the <code>linkagg lacp agg name</code> command.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative state of this dynamic aggregate group, which can be ENABLED or DISABLED. Configured through the <code>linkagg lacp agg admin-state</code> command.</td>
</tr>
<tr>
<td>Operational State</td>
<td>The operational state of this dynamic aggregate group, which can be UP or DOWN.</td>
</tr>
<tr>
<td>Aggregate Size</td>
<td>The number of links configured for this dynamic aggregate group.</td>
</tr>
<tr>
<td>Number of Selected Ports</td>
<td>The number of ports available to this dynamic aggregate group.</td>
</tr>
<tr>
<td>Number of Reserved Ports</td>
<td>The total number of ports reserved for use in link aggregation by this dynamic aggregate group.</td>
</tr>
<tr>
<td>Number of Attached Ports</td>
<td>The number of ports actually attached to this dynamic aggregate group.</td>
</tr>
<tr>
<td>Primary Port</td>
<td>The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate group is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.</td>
</tr>
<tr>
<td>Port Selection Hash</td>
<td>The hashing algorithm used to identify a specific traffic flow to hash.</td>
</tr>
<tr>
<td>Wait To Restore Time</td>
<td>The amount of time, in minutes, the switch waits to bring up a link aggregate that is attached to other links. Configured through the <code>linkagg lacp agg wait-to-restore-time</code> command.</td>
</tr>
<tr>
<td>MACAddress</td>
<td>The MAC address associated with the primary port.</td>
</tr>
<tr>
<td>Actor System Id</td>
<td>The MAC address of this dynamic aggregate group. Configured through the <code>linkagg lacp agg actor system-id</code> command.</td>
</tr>
<tr>
<td>Actor System Priority</td>
<td>The priority of this dynamic aggregate group. Configured through the <code>linkagg lacp agg actor system-priority</code> command.</td>
</tr>
<tr>
<td>Actor Admin Key</td>
<td>The administrative key associated with this dynamic aggregate group. Configured through the <code>linkagg lacp agg actor admin-key</code> command.</td>
</tr>
<tr>
<td>Actor Oper Key</td>
<td>The operational key associated with this dynamic aggregate group.</td>
</tr>
<tr>
<td>Partner System Id</td>
<td>The MAC address of the remote dynamic aggregate group. Configured through the <code>linkagg lacp agg partner system-id</code> command.</td>
</tr>
<tr>
<td>Partner System Priority</td>
<td>The priority of the remote system to which this dynamic aggregation group is attached. Configured through the <code>linkagg lacp agg partner system-priority</code> command.</td>
</tr>
<tr>
<td>Partner Admin Key</td>
<td>The administrative key for the remote partner of the dynamic aggregation. Configured through the <code>linkagg lacp agg partner admin-key</code> command.</td>
</tr>
<tr>
<td>Partner Oper Key</td>
<td>The operational key of the remote system to which the dynamic aggregation group is attached.</td>
</tr>
</tbody>
</table>
Release History

Release 7.1.1; command introduced.

Related Commands

- `linkagg static agg size`  Creates a static aggregate group.
- `linkagg static agg loopback`  Creates a static loopback aggregate group.
- `linkagg lacp agg size`  Creates a dynamic aggregate group.
- `show linkagg accounting`  Displays statistics for packet frames received and transmitted on link aggregate member ports.
- `show linkagg counters`  Displays statistics for the number of packet frames and errors received and transmitted on link aggregate member ports.

MIB Objects

- `alclnkagggAggTable`
  - `alclnkAggSize`
  - `alclnkaggAggNumber`
  - `alclnkaggAggDescr`
  - `alclnkaggAggName`
  - `alclnkaggAggLacpType`
  - `alclnkaggAggAdminState`
  - `alclnkaggAggOperState`
  - `alclnkaggAggNbrSelectedPorts`
  - `alclnkaggAggNbrAttachedPorts`
  - `alclnkaggAggOperPortIndex`
  - `alclnkaggAggPortSelectionHash`
  - `alclnkaggAggWTRTimer`
  - `alclnkaggAggMACAddress`
  - `alclnkaggAggActorSystemPriority`
  - `alclnkaggAggActorSystemID`
  - `alclnkaggAggPartnerAdminKey`
  - `alclnkaggAggActorAdminKey`
  - `alclnkaggAggActorOperKey`
  - `alclnkaggAggLocalRangeOperMin`
  - `alclnkaggAggLocalRangeOperMax`
  - `alclnkaggAggLocalRangeConfiguredMin`
  - `alclnkaggAggLocalRangeConfiguredMax`
  - `alclnkaggAggPeerRangeOperMin`
  - `alclnkaggAggPeerRangeOperMax`
  - `alclnkaggAggPartnerSystemID`
  - `alclnkaggAggPartnerSystemPriority`
  - `alclnkaggAggPartnerOperKey`
show linkagg port

Displays information about link aggregation ports.

```plaintext
show linkagg [agg agg_id[-agg_id2]] port [chassis/slot/port]
```

### Syntax Definitions

- `agg_id[-agg_id2]` The link aggregate ID number corresponding to the aggregate group. Use a hyphen to specify a range of IDs (10-20).
- `chassis` The chassis identifier.
- `slot/port` The slot and port number of the link aggregation port.

### Defaults

By default, all link aggregation ports are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If a particular slot or port is specified, the fields displayed depend upon whether the port belongs to a static aggregate group or a dynamic (LACP) aggregate group.

- If only a link aggregate or a range of link aggregates is specified along with the `agg` keyword, the ports and related information for only the specified link aggregate IDs are displayed.

### Examples

```plaintext
-> show linkagg port

Slot/Port Aggregate  SNMP Id   Status   Agg  Oper Link Prim
--------------------+----------+--------+----------+----+----+----+----+----
  2/1    Static        2001  ATTACHED     1  UP   UP   YES

-> show linkagg agg 1-5 port

Slot/Port Aggregate  SNMP Id   Status   Agg  Oper Link Prim
--------------------+----------+--------+----------+----+----+----+----+----
  1/16  Static  2016     CONFIGURED       1    UP   UP   YES
  1/17  Static  2017     CONFIGURED       2    UP   UP   NO
  3/1   Static  3001     CONFIGURED      3     UP   UP   NO
  3/2   Static  3045     CONFIGURED       4    UP   UP   NO
```

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 12-86
A port that belongs to a static aggregate is specified:

`-> show linkagg port 4/1`

**Static Aggregable Port**
- **SNMP Id**: 4001,
- **Slot/Port**: 4/1,
- **Administrative State**: ENABLED,
- **Operational State**: DOWN,
- **Port State**: CONFIGURED,
- **Link State**: DOWN,
- **Selected Agg Number**: 2,
- **Port position in the aggregate**: 0,
- **Primary port**: NONE

**output definitions**

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>The slot/port associated with the aggregate group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate</td>
<td>The type of aggregate group associated with the port, either Static or Dynamic.</td>
</tr>
<tr>
<td>SNMP Id</td>
<td>The SNMP ID associated with the aggregate group.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of the port, which can be CONFIGURED, PENDING, SELECTED, or RESERVED.</td>
</tr>
<tr>
<td>Agg</td>
<td>The number of the aggregate groups associated with this port.</td>
</tr>
<tr>
<td>Oper</td>
<td>The operational status of the port.</td>
</tr>
<tr>
<td>Link</td>
<td>The physical link status of the port.</td>
</tr>
<tr>
<td>Prim</td>
<td>Specifies if the port is the primary port of the aggregate. The primary port is the lowest numbered port in a link aggregate.</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>SNMP Id</th>
<th>The SNMP ID associated with this port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot/Port</td>
<td>The slot and port number.</td>
</tr>
<tr>
<td>Administrative State</td>
<td>The current administrative state of this port, which can be ENABLED or DISABLED.</td>
</tr>
<tr>
<td>Operational State</td>
<td>The current operational state of the port, which can be UP or DOWN.</td>
</tr>
<tr>
<td>Port State</td>
<td>The current operational state of the port, which can be CONFIGURED, PENDING, SELECTED, or RESERVED.</td>
</tr>
<tr>
<td>Link State</td>
<td>The current operational state of the link from this port to its remote partner, which can be UP or DOWN.</td>
</tr>
<tr>
<td>Selected Agg Number</td>
<td>The number associated with the static aggregate group to which the port is attached.</td>
</tr>
<tr>
<td>Port position in the aggregate</td>
<td>The rank of this port within the static aggregate group.</td>
</tr>
<tr>
<td>Primary Port</td>
<td>The port number of the first port to join this static aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.</td>
</tr>
</tbody>
</table>
A port that belongs to a static link aggregate is specified:

```plaintext
-> show linkagg agg 1
```

### Static Aggregate

- **SNMP Id**: 40000001,
- **Aggregate Number**: 1,
- **SNMP Descriptor**: Omnichannel Aggregate Number 1 ref 40000001 size 4,
- **Name**: ,
- **Admin State**: ENABLED,
- **Operational State**: DOWN,
- **Aggregate Size**: 4,
- **Number of Selected Ports**: 0,
- **Number of Reserved Ports**: 0,
- **Number of Attached Ports**: 0,
- **Primary Port**: NONE

A port that belongs to a dynamic aggregate is specified:

```plaintext
-> show linkagg port 2/1
```

### Dynamic Aggregable Port

- **SNMP Id**: 2001,
- **Slot/Port**: 2/1,
- **Administrative State**: ENABLED,
- **Operational State**: DOWN,
- **Port State**: CONFIGURED,
- **Link State**: DOWN,
- **Selected Agg Number**: NONE,
- **Primary port**: UNKNOWN

### LACP

- **Actor System Priority**: 10,
- **Actor System Id**: [00:d0:95:6a:78:3a],
- **Actor Admin Key**: 8,
- **Actor Oper Key**: 8,
- **Partner Admin System Priority**: 20,
- **Partner Oper System Priority**: 20,
- **Partner Admin System Id**: [00:00:00:00:00:00],
- **Partner Oper System Id**: [00:00:00:00:00:00],
- **Partner Admin Key**: 8,
- **Partner Oper Key**: 0,
- **Attached Agg Id**: 0,
- **Actor Port**: 7,
- **Actor Port Priority**: 15,
- **Partner Admin Port**: 0,
- **Partner Oper Port**: 0,
- **Partner Admin Port Priority**: 0,
- **Partner Oper Port Priority**: 0,
- **Actor Admin State**: act1.tim1.agg1.syn0.col1.dis0.def1.exp0
- **Actor Oper State**: act1.tim1.agg1.syn0.col1.dis1.def1.exp0
- **Partner Admin State**: act0.tim0.agg1.syn1.col1.dis1.def1.exp0
- **Partner Oper State**: act0.tim0.agg1.syn1.col1.dis1.def1.exp0

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Id</td>
<td>The SNMP ID associated with this port.</td>
</tr>
<tr>
<td>Slot/Port</td>
<td>The slot and port number.</td>
</tr>
<tr>
<td>Administrative State</td>
<td>The current administrative state of this port, which can be <strong>ENABLED</strong> or <strong>DISABLED</strong>.</td>
</tr>
</tbody>
</table>
### Output Definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operational State</strong></td>
<td>The current operational state of the port, which can be <strong>UP</strong> or <strong>DOWN</strong>.</td>
</tr>
<tr>
<td><strong>Port State</strong></td>
<td>The current operational state of the port, which can be <strong>CONFIGURED</strong>, <strong>PENDING</strong>, <strong>SELECTED</strong>, or <strong>AGGREGATED</strong>.</td>
</tr>
<tr>
<td><strong>Link State</strong></td>
<td>The current operational state of the link from this port to its remote partner, which can be <strong>UP</strong> or <strong>DOWN</strong>.</td>
</tr>
<tr>
<td><strong>Selected Agg Number</strong></td>
<td>The number associated with the dynamic aggregate group to which the port is attached.</td>
</tr>
<tr>
<td><strong>Primary Port</strong></td>
<td>The port number of the first port to join this dynamic aggregate group. If the first port to join the aggregate is no longer part of the aggregate group, the switch automatically assigns another port in the aggregate group to be the primary port.</td>
</tr>
<tr>
<td><strong>Actor System Priority</strong></td>
<td>The actor system priority of this port. Configured through the <code>linkagg lACP port actor system-priority</code> command.</td>
</tr>
<tr>
<td><strong>Actor System Id</strong></td>
<td>The actor system ID (i.e., MAC address) of this port. Configured through the <code>linkagg lACP port actor system-id</code> command.</td>
</tr>
<tr>
<td><strong>Actor Admin Key</strong></td>
<td>The actor administrative key value for this port. Configured through the <code>linkagg lACP port actor admin-key</code> command.</td>
</tr>
<tr>
<td><strong>Actor Oper Key</strong></td>
<td>The actor operational key associated with this port.</td>
</tr>
<tr>
<td><strong>Partner Admin System Priority</strong></td>
<td>The administrative priority of the remote system to which this port is attached. Configured through the <code>linkagg lACP port partner admin system-priority</code> command.</td>
</tr>
<tr>
<td><strong>Partner Oper System Priority</strong></td>
<td>The operational priority of the remote system to which this port is attached.</td>
</tr>
<tr>
<td><strong>Partner Admin System Id</strong></td>
<td>The administrative MAC address associated with the system ID of a remote partner. This value is used along with Partner Admin System Priority, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. Configured through the <code>linkagg lACP port partner admin system-id</code> command.</td>
</tr>
<tr>
<td><strong>Partner Oper System Id</strong></td>
<td>The MAC address that corresponds to the system ID of the remote partner.</td>
</tr>
<tr>
<td><strong>Partner Admin Key</strong></td>
<td>The administrative value of the key for the remote partner. This value is used along with Partner Admin System Priority, Partner Admin System, Partner Admin Port, and Partner Admin Port Priority to manually configure aggregation. Configured through the <code>linkagg lACP port partner admin-key</code> command.</td>
</tr>
<tr>
<td><strong>Partner Oper Key</strong></td>
<td>The current operational value of the key for the protocol partner.</td>
</tr>
<tr>
<td><strong>Attached Agg ID</strong></td>
<td>The ID of the aggregate group that the port has attached itself to. A value of zero indicates that the port is not attached to an aggregate group.</td>
</tr>
<tr>
<td><strong>Actor Port</strong></td>
<td>The port number locally assigned to this port.</td>
</tr>
<tr>
<td><strong>Actor Port Priority</strong></td>
<td>The actor priority value assigned to the port. Configured through the <code>linkagg lACP port actor port priority</code> command.</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Admin Port</td>
<td>The administrative value of the port number for the protocol partner. This value is used along with Partner Admin System Priority, Partner Admin System ID, Partner Admin Key, and Partner Admin Port Priority to manually configure aggregation. Configured through the <code>linkagg lacp port partner admin-port</code> command.</td>
</tr>
<tr>
<td>Partner Oper Port</td>
<td>The operational port number assigned to the port by the protocol partner.</td>
</tr>
<tr>
<td>Partner Admin Port Priority</td>
<td>The administrative port priority of the protocol partner. This value is used along with Partner Admin System Priority, Partner Admin System ID, and Partner Admin Key to manually configure aggregation. Configured through the <code>linkagg lacp port partner admin port-priority</code> command.</td>
</tr>
<tr>
<td>Partner Oper Port Priority</td>
<td>The priority value assigned to the this port by the partner.</td>
</tr>
<tr>
<td>Actor Admin State</td>
<td>The administrative state of the port. Configured through the <code>linkagg lacp port actor admin-state</code> command.</td>
</tr>
<tr>
<td>Actor Oper State</td>
<td>The current operational state of the port.</td>
</tr>
<tr>
<td>Partner Admin State</td>
<td>The administrative state of the partner port. Configured through the <code>linkagg lacp agg partner admin-state</code> command.</td>
</tr>
<tr>
<td>Partner Oper State</td>
<td>The current operational state of the partner port.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `linkagg static port agg`  
  Configures a slot and port for a static aggregate group.
- `linkagg lacp port actor admin-key`  
  Configures a slot and port for a dynamic aggregate group.
- `show linkagg`  
  Displays information about static and dynamic (LACP) aggregate groups.
MIB Objects

alclnkaggAggPortTable
   alclnkaggAggPortActorSystem
   alclnkaggAggPortActorSystemPriority
   alclnkaggAggPortActorSystemID
   alclnkaggAggPortActorAdminKey
   alclnkaggAggPortActorOperKey
   alclnkaggAggPortPartnerAdminSystemPriority
   alclnkaggAggPortPartnerOperSystemPriority
   alclnkaggAggPortPartnerAdminSystemID
   alclnkaggAggPortPartnerOperSystemID
   alclnkaggAggPortPartnerAdminKey
   alclnkaggAggPortPartnerOperKey
   alclnkaggAggPortSelectedAggID
   alclnkaggAggPortAttachedAggID
   alclnkaggAggPortActorPort
   alclnkaggAggPortActorPortPriority
   alclnkaggAggPortPartnerAdminPort
   alclnkaggAggPortPartnerOperPort
   alclnkaggAggPortPartnerAdminPortPriority
   alclnkaggAggPortPartnerOperPortPriority
   alclnkaggAggPortActorAdminState
   alclnkaggAggPortActorOperState
   alclnkaggAggPortPartnerAdminState
   alclnkaggAggPortPartnerOperState
show linkagg accounting

Displays statistics collected for packets transmitted and received on link aggregate ports.

show linkagg accounting

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
- Statistics are displayed for all link aggregate IDs configured on the switch.
- Statistics are collected for undersized and oversized packets, packets of a certain size, and Jabber frames.

Examples

-> show linkagg accounting

Link Agg 10
rx undersize packets = 0
tx undersize packets = 0
rx oversize packets = 0
tx oversize packets = 0
rx packets 64 = 3073753
rx packets 65_127 = 678698
rx packets 128_255 = 21616
rx packets 256_511 = 21062
rx packets 512_1023 = 2
rx packets 1024_1518 = 84
rx packets 1519_4095 = 0
rx packets 4096_9216 = 0
rx jabber frames = 0

Release History
Release 8.3.1; command introduced.
Related Commands

**show linkagg counters**
Displays statistics collected for the type and number of packets transmitted and received on link aggregate ports.

**show linkagg traffic**
Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.

**clear linkagg-statistics**
Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

- `lnkaggAggIdAccountTable`
  - `alcRxUndersize`
  - `alcTxUndersize`
  - `alcRxOversize`
  - `alcTxOversize`
  - `alcRxPackets64`
  - `alcRxPackets127`
  - `alcRxPackets255`
  - `alcRxPackets511`
  - `alcRxPackets1023`
  - `alcRxPackets1518`
  - `alcRxPackets4095`
  - `alcRxPackets9216`
  - `alcRxJabberFrames`
show linkagg counters

Displays statistics collected for the type and number of packet frames transmitted and received on link aggregate ports.

show linkagg counters [errors]

Syntax Definitions

errors Display the number of errors received on the link aggregate member ports.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Statistics are displayed (in bytes or frame count) for all link aggregate IDs configured on the switch.
- Error statistics include the number of alignment, frame check (FCS), received, and transmitted errors.

Examples

```
-> show linkagg counters
Link Agg 10
InOctets    = 54367578586897979
OutOctets   = 5.78E19
InUcastPkts = 55654265276
OutUcastPkts= 5.78E20
InMcastPkts = 58767867868768777
OutMcastPkts= 5465758756856
InBcastPkts = 576567567567567576
OutBcastPkts= 786876
InPause frames = 567798768768767
OutPause frames= 786876

-> show linkagg counters errors
Link Agg 10
Alignments Errors = 6.45E13
FCS Errors        = 7.65E12
```
IfInErrors = 6435346
IfOutErrors = 5543

**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- **show linkagg accounting**  Displays statistics collected for packets transmitted and received on link aggregate ports.
- **show linkagg traffic**  Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.
- **clear linkagg-statistics**  Clears statistics for all link aggregates or for specific aggregate IDs.

**MIB Objects**

alcInAggIdCounterTable
alcInOctets
alcOutOctets
alcInUcastPkts
alcOutUcastPkts
alcInMcastPkts
alcOutMcastPkts
alcInBcastPkts
alcOutBcastPkts
alcInPauseFrames
alcOutPauseFrames
show linkagg traffic

Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Statistics are displayed for all link aggregate IDs configured on the switch.

Examples

-> show linkagg traffic

<table>
<thead>
<tr>
<th>Agg</th>
<th>Input Packets</th>
<th>Input Bytes</th>
<th>Output Packets</th>
<th>Output Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>322</td>
<td>20624</td>
<td>5125</td>
<td>347216</td>
</tr>
<tr>
<td>20</td>
<td>456</td>
<td>30620</td>
<td>6133</td>
<td>397764</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command introduced.
Related Commands

**show linkagg accounting**
Displays statistics collected for packets transmitted and received on link aggregate ports.

**show linkagg counters**
Displays statistics collected for the type and number of packets transmitted and received on link aggregate ports.

**clear linkagg-statistics**
Clears statistics for all link aggregates or for specific aggregate IDs.

MIB Objects

alclnkaggAggIdTrafficTable
  alcInputPackets
  alcInputBytes
  alcOutputPackets
  alcOutputBytes
clear linkagg-statistics

Clears statistics for all link aggregates or for a specific aggregate ID or range of IDs.

clear linkagg-statistics [agg agg_id[-agg_id2]]

**Syntax Definitions**

`agg_id[-agg_id2]`  
The link aggregate ID number corresponding to the static aggregate group. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

By default, statistics are cleared for all link aggregates.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command sets all statistic counters to zero.

**Examples**

- `-> clear linkagg-statistics`
- `-> clear linkagg-statistics agg 10`
- `-> clear linkagg-statistics agg 11-15`

**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `show linkagg accounting`  
  Displays statistics collected for packets transmitted and received on link aggregate ports.
- `show linkagg counters`  
  Displays statistics collected for the type and number of packets transmitted and received on link aggregate ports.
- `show linkagg traffic`  
  Displays the total number of packets and bytes that are received and transmitted on link aggregate ports.
MIB Objects

alclnkaggAggPortStatsTable
  alclnkaggAggPortStatsLACPDUssRx
  alclnkaggAggPortStatsMarkerPDUssRx
  alclnkaggAggPortStatsMarkerResponsePDUssRx
  alclnkaggAggPortStatsUnknownRx
  alclnkaggAggPortStatsIllegalRx
  alclnkaggAggPortStatsLACPDUssTx
  alclnkaggAggPortStatsMarkerPDUssTx
  alclnkaggAggPortStatsMarkerResponsePDUssTx
13 Virtual Chassis Commands

A Virtual Chassis is a group of switches managed through a single management IP address and that behave as a single bridge or router. It provides both node level and link level redundancy for devices connecting to the aggregation layer via dual-homed standard 802.3ad link aggregation mechanisms. The use of Virtual Chassis provides node level redundancy without the need to use redundancy protocols such as STP and VRRP between the edge and the aggregation/core layer.

MIB information for the Virtual Chassis commands is as follows:

- **Filename**: ALCATEL-IND1-VIRTUAL-CHASSIS-MIB.mib
  - **Module**: alcatelIND1VirtualChassisMIB

- **Filename**: ALCATEL-IND1-VC-SPLIT-PROTECTION-MIB.mib
  - **Module**: alaVCSPMIB
A summary of available commands is listed here:

<table>
<thead>
<tr>
<th>Virtual Chassis Commands</th>
<th>virtual-chassis configured-chassis-id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>virtual-chassis chassis-group</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis configured-chassis-priority</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis configured-control-vlan</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis configured-hello-interval</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis vf-link create</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis vf-link member-port</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis vf-link default-vlan</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis hello-interval</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis shutdown</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis vf-link-mode</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis auto-vf-link-port</td>
</tr>
<tr>
<td></td>
<td>vc-takeover</td>
</tr>
<tr>
<td></td>
<td>ssh-chassis</td>
</tr>
<tr>
<td></td>
<td>convert configuration</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis topology</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis consistency</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis vf-link</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis auto-vf-link-port</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis chassis-reset-list</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis slot-reset-list</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis consistency</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis neighbors</td>
</tr>
<tr>
<td></td>
<td>show configuration vcm-snapshot chassis-id</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Virtual Chassis Split Protection Commands</th>
<th>virtual-chassis split-protection admin-state</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>virtual-chassis split-protection linkagg</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis split-protection guard-timer</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis split-protection helper admin-state</td>
</tr>
<tr>
<td></td>
<td>virtual-chassis split-protection helper linkagg</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis split-protection status</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis split-protection vc-units</td>
</tr>
<tr>
<td></td>
<td>show virtual-chassis split-protection helper status</td>
</tr>
</tbody>
</table>
**virtual-chassis configured-chassis-id**

Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual-chassis mode.

```
virtual-chassis [chassis-id oper_chassis] configured-chassis-id config_chassis
no virtual-chassis [chassis-id oper_chassis] configured-chassis-id config_chassis
```

**Syntax Definitions**

- `oper_chassis`  
  The operational/current chassis ID number.

- `config_chassis`  
  The configured/next chassis ID number.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>oper_chassis</code></td>
<td>0 (standalone mode; no virtual chassis operation is allowed)</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- Use the `no` form of this command to change the chassis ID back to “0” (the default). When the chassis ID is set to “0”, the switch operates in standalone mode and all virtual chassis related configuration commands are no longer active for the switch.
- The operational chassis identifier parameter is only optional when the switch is running in standalone mode or at start up time, within the `vcsetup.cfg`, when the switch is coming up in virtual chassis mode. The same restrictions apply to the no form of the command.
- The operational chassis identifier is a mandatory parameter whenever the system is running in virtual chassis mode. This prevents modifying the chassis identifier of all switches at the same time and causing a duplicate chassis identifier.
- Two switches that have the same chassis identifier are not allowed to operate in virtual chassis mode. If a duplicate chassis identifier is detected one of the switches will be in an inconsistent role and its status will be set to Duplicate-Chassis-ID.
- The configured chassis identifier will only take effect after the next reboot of the target chassis.
• Virtual chassis is only supported between two switches of the same type. For example, virtual chassis is not supported between an OmniSwitch 6860 and an OmniSwitch 6900.

• The no form of this command can only be used if there are no VFLs configured on the switch.

• Snapshots produced through the show configuration vcm-snapshot, show configuration snapshot virtual chassis or write memory commands always include the operational chassis identifier.

Examples
-> virtual-chassis configured-chassis-id 1 //Standalone mode
-> virtual-chassis chassis-id 0 configured-chassis-id 1
-> no virtual-chassis chassis-id 0 configured-chassis-id
-> no virtual-chassis configured-chassis-id

Release History
Release 7.3.1; command introduced.

Related Commands
vc-takeover Converts an existing standalone configuration to a virtual chassis configuration.

show virtual-chassis consistency Displays the system level mandatory consistency parameters of both the local and peer switches.

show virtual-chassis topology Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

virtualChassisGlobalTable
  virtualChassisOperChasId
  virtualChassisConfigChassisId
virtual-chassis chassis-group

Assigns a globally unique chassis group identifier to a chassis. Each peer switch in a virtual chassis domain must use the same group ID number. The group ID number uniquely identifies switches operating in the same virtual chassis.

`virtual-chassis [chassis-id oper_chassis] chassis-group group`

**Syntax Definitions**

- `oper_chassis`: The operational/current chassis ID number.
- `group`: Virtual chassis group identifier (0-255), which is used to identify a group of chassis belonging to the same virtual chassis.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>group</td>
<td>Derived from last byte of Master chassis MAC address</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- Each virtual chassis domain must use a different group ID number to differentiate the domain within the network environment.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches is running in virtual chassis mode the chassis group can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.
- When a set of switches is running in virtual chassis mode the chassis group can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.
- It is strongly recommended that the same chassis group value is set for all switches that will participate on the same virtual chassis group. Failure to adhere to this recommendation followed by a system reset will prevent the switches whose values are different from joining the same virtual chassis group.
• When determining the chassis group ID the last byte of the Master chassis MAC address is used. For example, if the Master's MAC address is xx:xx:xx:xx:xx:7e, the chassis group will be 126 (equivalent to hex 7e).

**Examples**

- virtual-chassis chassis-id 1 chassis-group 10
- virtual-chassis chassid-id 0 chassis-group 10
- virtual-chassis chassis-group 10 // All switches

**Release History**

Release 7.3.1; command introduced.
Release 7.3.4; Chassis group ID based on Master MAC address introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vc-takeover</td>
<td>Converts an existing standalone configuration to a virtual chassis configuration</td>
</tr>
<tr>
<td>show virtual-chassis consistency</td>
<td>Displays the system level mandatory consistency parameters of both the local and peer switches.</td>
</tr>
<tr>
<td>show virtual-chassis topology</td>
<td>Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.</td>
</tr>
</tbody>
</table>

**MIB Objects**

virtualChassisGlobalTable
  virtualChassisOperChasID
  virtualChassisGroup
**virtual-chassis configured-chassis-priority**

Sets the configured chassis priority for a chassis specified by its operational chassis identifier.

```
virtual-chassis [chassis-id oper_chassis] configured-chassis-priority priority
```

**Syntax Definitions**

- **oper_chassis**: The operational/current chassis ID number.
- **priority**: Configured chassis priority (0-255) which defines the user preference above all other election criteria, for the target chassis to become the master of the virtual chassis.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>OS6900-Q32 - 120</td>
</tr>
<tr>
<td></td>
<td>All others - 100</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- The greatest configured-chassis-priority will become the Master chassis. Without setting this value the smallest chassis identifier becomes the key parameter used to determine which switch will become the Master.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- The configured chassis priority will only take effect after the next reboot of the target switch.

**Examples**

**Standalone mode:**
- `-> virtual-chassis chassis-priority 50`
- `-> virtual-chassis chassis-id 0 chassis-priority 50`

**All switches:**
- `-> virtual-chassis configured-chassis-priority 50`
- `-> virtual-chassis chassid-id 0 configured-chassis-priority 50`
Chassis 2 only:

`virtual-chassis chassis-id 2 configured-chassis-priority 75` //Chassis 2 only

**Release History**

Release 7.3.1.R01; command introduced.

**Related Commands**

- **vc-takeover**: Converts an existing standalone configuration to a virtual chassis configuration.
- **show virtual-chassis consistency**: Displays the system level mandatory consistency parameters of both the local and peer switches.
- **show virtual-chassis topology**: Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

**MIB Objects**

- `virtualChassisGlobalTable`
  - `virtualChassisOperChasID`
  - `virtualChassisConfigPriority`
**virtual-chassis configured-control-vlan**

Sets the configured control VLAN for a chassis specified by its operational chassis identifier.

```
virtual-chassis [chassis-id oper_chassis] configured-control-vlan vlan
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>oper_chassis</code></td>
<td>The operational/current chassis ID number.</td>
</tr>
<tr>
<td><code>vlan</code></td>
<td>Configured/next virtual chassis control VLAN (2-4094), which is used for all internal control communication between switches over the VFL.</td>
</tr>
</tbody>
</table>

**Defaults**

```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan</code></td>
<td>4094</td>
</tr>
</tbody>
</table>
```

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- This configured control VLAN will only take effect after the next reboot of the target switch.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches in running in virtual chassis mode, the configured control VLAN can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.
- When a set of switches in running in virtual chassis mode, the configured control VLAN can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.
- It is strongly recommended that the value is for all switches that will participate in the same virtual chassis topology.
Examples

Standalone mode:
-> virtual-chassis configured-control-vlan 10
-> virtual-chassis chassis-id 0 configured-control-vlan 10

All switches:
-> virtual-chassis configured-control-vlan 10
-> virtual-chassis chassis-id 0 configured-control-vlan 10

Release History

Release 7.3.1; command introduced.

Related Commands

vc-takeover
Converts an existing standalone configuration to a virtual chassis configuration.

show virtual-chassis consistency
Displays the system level mandatory consistency parameters of both the local and peer switches.

show virtual-chassis topology
Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

virtualChassisGlobalTable
  virtualChassisOperChasID
  virtualChassisConfigControlVlan
virtual-chassis configured-hello-interval

Sets the virtual chassis configured hello interval parameter on the switch. Hello packets are sent periodically on the virtual fabric link (VFL) interfaces to establish a relationship and bidirectional communication between virtual chassis switches. The hello interval value determines how often these packets are sent.

```
virtual-chassis [chassis-id oper_chassis] configured-hello-interval hello
```

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>oper_chassis</td>
<td>The operational/current chassis ID number.</td>
</tr>
<tr>
<td>hello</td>
<td>Configured/next virtual chassis hello interval in seconds (1-10), which defines how frequently the keep-alives related to the virtual chassis hello protocol are exchanged over the VFL links.</td>
</tr>
</tbody>
</table>

Defaults

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello</td>
<td>5</td>
</tr>
</tbody>
</table>
```

Platforms Supported

Not supported in this release.

Usage Guidelines

- The configured value will only take effect after the next reboot of the target switch.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches is running in virtual chassis mode, the configured hello interval can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.
- When a set of switches is running in virtual chassis mode, the configured hello interval can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.
- The hello timeout is a fixed value and defined as 120 seconds. This is the minimum time interval that a switch will wait without receiving any hello packets from a peer switch before declaring that the adjacency towards that switch was lost.
- It is strongly recommended that the hello interval be the same for all switches that will participate in the same virtual chassis topology.

Examples

Standalone mode:

```
-> virtual-chassis configured-hello-interval 10
-> virtual-chassis chassis-id 0 configured-hello-interval 10
```
All switches:

-> virtual-chassis configured-hello-interval 10
-> virtual-chassis chassis-id 0 configured-hello-interval 10

**Release History**

Release 7.3.1; command introduced.
Release 7.3.3; command deprecated.

**Related Commands**

- **vc-taking** Converts an existing standalone configuration to a virtual chassis configuration.
- **show virtual-chassis consistency** Displays the system level mandatory consistency parameters of both the local and peer switches.
- **show virtual-chassis topology** Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

**MIB Objects**

virtualChassisGlobalTable
  virtualChassisOperChasID
  virtualChassisConfigHelloInterval
**virtual-chassis vf-link create**

Configures a virtual fabric link (VFL) between two peer switches. A VFL is required to enable the virtual chassis operation between the two switches.

```
virtual-chassis [chassis-id oper_chassis] vf-link vfl_id create
```

```
no virtual-chassis [chassis-id oper_chassis] vf-link vfl_id
```

---

**Syntax Definitions**

- `oper_chassis`: The operational/current chassis ID number.
- `vfl_id`: The VFL link identifier (0).

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.

- Although a virtual fabric link can be configured while the switch is running either in standalone or virtual chassis mode, a VFL can only become operational when the chassis operates in virtual chassis mode.

- Use the no form of this command to remove the VFL configuration from the switch.

- Although the switch supports runtime configuration of the VFL and its member ports, configuring the VFL at the same time as the chassis identifier is configured and before rebooting the switch is recommended.

- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.

- This command is valid only when the VFL mode is set to static.

- Platforms that do not support static VFLs do not support this command.

---

**Examples**

```
-> virtual-chassis vf-link 0 create
-> virtual-chassis chassis-id 0 vf-link 0 create
-> no virtual-chassis vf-link 0
```
Virtual Chassis Commands

virtual-chassis vf-link create

- no virtual-chassis chassis-id 0 vf-link 0
- virtual-chassis chassis-id 1 vf-link 0 create
- virtual-chassis chassis-id 2 vf-link 0 create
- no virtual-chassis chassis-id 1 vf-link 0
- no virtual-chassis chassis-id 2 vf-link 0

Release History

Release 7.3.1; command introduced.

Related Commands

vc-takeover
Converts an existing standalone configuration to a virtual chassis configuration.

show virtual-chassis consistency
Displays the system level mandatory consistency parameters of both the local and peer switches.

show virtual-chassis vf-link
Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

virtualChassisLinkTable
virtualChassisOperChasID
virtualChassisLinkID
virtualChassisVflRowStatus
**virtual-chassis vf-link member-port**

Adds member ports to a given virtual fabric link (VFL).

```plaintext
virtual-chassis [chassis-id oper_chassis] vf-link vfl_id member-port [oper_chassis/slot/port]
no virtual-chassis [chassis-id oper_chassis] vf-link vfl_id member-port [oper_chassis/slot/port]
```

**Syntax Definitions**

- `oper_chassis` The operational/current chassis ID number.
- `vfl_id` The VFL link identifier (0).
- `oper_chassis/slot/port` The operational chassis identifier, slot, and port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- Although virtual-fabric link (VFL) member ports can be configured while the switch is running either in standalone or virtual chassis mode, a configured virtual-fabric link (VFL) member port can only become operational when the chassis operates in virtual chassis mode.
- Use the no form of this command to remove a member port from the virtual-fabric link (VFL).
- When a switch is running in virtual chassis mode, a virtual-fabric link member port must be fully specified including `oper_chassis/slot/port`.
- Although the switch supports runtime configuration of the virtual-fabric link (VFL) and its member ports, configuring the virtual-fabric link (VFL) at the same time as the chassis identifier is configured and before rebooting the switch is recommended.
- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.
- When a set of switches in running in virtual chassis mode, a virtual-fabric link (VFL) member ports can only be created or removed exactly in one switch at a time. In other words, we are not allowed to create or remove a virtual chassis link member port with a system operating in virtual chassis mode if no operational chassis identifier is provided or if the value zero is specified.
- A maximum of 16 member ports can be added or assigned to each virtual-fabric link (VFL).
• All virtual-fabric link (VFL) member ports must operate at the same speed.

• Only interfaces that operate at 10G speed or above can be added or assigned to a virtual-fabric link. (Note: 10GBaseT ports cannot be assigned to a VFL).

• Only interfaces operating in full-duplex mode can be added or assigned to a virtual-fabric link.

• It is recommended to configure virtual-fabric link (VFL) member ports across multiple network interface modules (NI) for resilience reasons.

• Virtual-fabric link (VFL) member ports can only be configured on interfaces that are fixed ports, network ports or priority flow control enabled ports. For instance, interfaces configured as Q-tag ports or ERP ports cannot be configured as virtual-fabric link member ports.

• When a switch is running in virtual chassis mode, the interface related to the last active virtual-fabric link member port cannot be administratively disabled.

• When a switch is running in virtual chassis mode, the last active virtual-fabric link member port cannot be deleted using the no form of the present command.

• When a switch is running in virtual chassis mode, the network interface module (NI) that hosts the last active virtual-fabric link member port cannot be administratively reset or powered off.

• This command is valid only when the VFL mode is set to static.

• Platforms that do not support static VFLs do not support this command.

Examples

-> virtual-chassis chassis-id 0 vf-link 1 member-port 0/1/1
-> virtual-chassis chassis-id 0 vf-link 1 member-port 0/2/1
-> virtual-chassis chassis-id 1 vf-link 1 member-port 1/1/1
-> no virtual-chassis chassis-id 0 vf-link 1 member-port 0/1/1
-> no virtual-chassis chassis-id 0 vf-link 1 member-port 0/2/1
-> no virtual-chassis chassis-id 1 vf-link 1 member-port 1/1/1

Release History

Release 7.3.1; command introduced.

Related Commands

show virtual-chassis consistency
Displays information about the virtual fabric link on the switch.

show virtual-chassis chassis-reset-list
Displays detailed information about the virtual fabric link member ports on the switch.

show virtual-chassis vf-link
Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

virtualChassisLinkTable
virtualChassisOperChasID
virtualChassisLinkId
virtualChassisVflMemberPortIfindex
virtualChassisVflMemberPortRowStatus
**virtual-chassis vf-link default-vlan**

Configures the default VLAN for the virtual fabric link (VFL).

```
virtual-chassis [chassis-id oper_chassis] vf-link vfl_id default-vlan vlan
```

```
no virtual-chassis [chassis-id oper_chassis] vf-link vfl_id default-vlan
```

### Syntax Definitions

- **oper_chassis**: The operational/current chassis ID number.
- **vfl_id**: The VFL link identifier (0).
- **vlan**: The default VLAN (1-4094) for the specified VFL.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

Not supported in this release.

### Usage Guidelines

- This configured VLAN will become the default untagged VLAN for the VFL.

- Although the switch supports runtime configuration of the virtual-fabric link (VFL) and its member ports, configuring the virtual-fabric link (VFL) at the same time as the chassis identifier is configured and before rebooting the switch is recommended.

- Use the `no` form of this command to set the default VLAN back to 1.

- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.

- When a set of switches is running in virtual chassis mode, a virtual-fabric link (VFL) default VLAN can only be configured exactly in one switch at a time. In other words, we are not allowed to configured the virtual chassis link default VLAN with a system operating in virtual chassis mode if no operational chassis identifier is provided or if the value zero is specified.

- It is strongly recommended that the user set the same value of default VLAN for all virtual-fabric links on all switches that will participate on the same virtual chassis topology. Failure to adhere to this recommendation may cause end to end connectivity problems in the network.
Examples

Standalone mode:
-> virtual-chassis vf-link 0 default-vlan 5
-> virtual-chassis chassis-id 0 vf-link 0 default-vlan 5
-> no virtual-chassis vf-link 0 default-vlan
-> no virtual-chassis chassis-id 0 vf-link 0 default-vlan

Chassis 1:
-> virtual-chassis chassis-id 1 vf-link 0 default-vlan 5
-> no virtual-chassis chassis-id 1 vf-link 0 default-vlan

Release History

Release 7.3.1; command introduced.
Release 7.3.4; command deprecated.

Related Commands

show virtual-chassis vf-link Displays information about the virtual fabric link on the switch.

MIB Objects

virtualChassisLinkTable
  virtualChassisOperChasID
  virtualChassisLinkID
  virtualChassisLinkOperDefaultVlan
**virtual-chassis hello-interval**

Sets the virtual chassis configured hello interval parameter on the chassis. Hello packets are sent periodically on the virtual fabric link (VFL) interfaces to establish a relationship and bidirectional communication between virtual chassis switches. The hello interval value determines how often these packets are sent.

```
virtual-chassis [chassis-id oper_chassis] hello-interval hello
```

**Syntax Definitions**

- **oper_chassis**: The operational/current chassis ID number
- **hello**: The operational/current virtual chassis hello interval in seconds (1–2000), which defines how frequently the keep-alives related to the virtual chassis hello protocol are exchanged over the VFL links.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello</td>
<td>10 (6900 all models) 15 (6360, 6560, 6570M, 6860, 6860N) 60 (9900)</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.

- If no operational chassis identifier is specified or if the value specified is zero, then the value is applied to all switches in the virtual chassis.

- When a set of switches is running in virtual chassis mode, the configured hello interval can only be configured with exactly the same value as the master chassis when the configuration applies to a single and specific switch.

- When a set of switches is running in virtual chassis mode, the hello interval can be configured with any value within the valid range as long as the configuration applies to all switches at the same time.

- It is strongly recommended that the hello interval be the same for all switches that will participate in the same virtual chassis topology.
Examples

Standalone mode:
-> virtual-chassis hello-interval 10
-> virtual-chassis chassis-id 0 hello-interval 10

Virtual chassis mode:
-> virtual-chassis hello-interval 10  //All chassis
-> virtual-chassis chassis-id 2 configured-hello-interval 10  //Chassis 2 only

Release History

Release 7.3.3; command introduced.

Related Commands

vc-takeover  Converts an existing standalone configuration to a virtual chassis configuration.
show virtual-chassis consistency  Displays the system level mandatory consistency parameters of both the local and peer switches.
show virtual-chassis topology  Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

virtualChassisGlobalTable
  virtualChassisOperChasID
  virtualChassisOperHelloInterval
virtual-chassis shutdown

Disables all front-panel port including the user ports and all the VFL member ports on a chassis isolating the chassis from the rest of the virtual chassis topology.

virtual-chassis shutdown [chassis-id oper_chassis]

Syntax Definitions

oper_chassis The operational/current chassis ID number.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• The OS6900-X48C4E does not support a Virtual Chassis configuration.

• This command will disable all front panel ports, including the user ports and all virtual-fabric link (VFL) member ports on the specified switch.

• After running this command remote access to the target switch is only possible through the local EMP port on that switch.

• The target switch must be reloaded to bring its ports back to an operational state.

• This command is only functional when executed through the master chassis of a system operating in virtual chassis mode.

• After the shutdown command is executed, the target switch assumes the role of master and remains isolated from all other switches in the virtual chassis topology.

Examples

→ virtual-chassis shutdown chassis-id 2

Release History

Release 7.3.1; command introduced.
Related Commands

**show virtual-chassis consistency**
Displays the system level mandatory consistency parameters of both the local and peer switches.

MIB Objects

N/A
**virtual-chassis vf-link-mode**

Configures the Virtual Chassis mode. Virtual Chassis mode determines whether the VFLs are created automatically or statically.

```
virtual-chassis vf-link-mode {static | auto}
```

**Syntax Definitions**

N/A

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vf-link-mode</td>
<td><strong>auto</strong> (if no vcsetup.cfg file exists).</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- If the chassis boots without a `vcsetup.cfg` file the mode defaults to auto.
- If the chassis boots with a `vcsetup.cfg` file and the ‘virtual-chassis vf-link-mode’ CLI does not exist, the mode will be set to static. Otherwise, the mode will be set as configured in the `vcsetup.cfg` file.
- Changing the mode is only allowed for all chassis or the local chassis. Specific chassis configuration is not allowed.
- Platforms that do not support static VFLs do not support this command.

**Examples**

```
-> virtual-chassis vf-link-mode auto
-> virtual-chassis vf-link-mode static
```

**Release History**

Release 7.3.4; command introduced.
Related Commands

**show virtual-chassis vf-link**  
Displays a summary of the configured and operational parameters related to the virtual fabric link on the switch.

MIB Objects

virtualChassisGlobalTable
- virtualChassisOperChasID
- virtualChassisVf1Mode
**virtual-chassis auto-vf-link-port**

Configures the port to be an automatic VFL port.

```
[no] virtual-chassis auto-vf-link-port chassis/slot/port
```

### Syntax Definitions

- **chassis/slot/port**
  The operational chassis ID, slot, and port.

### Defaults

<table>
<thead>
<tr>
<th>chassis type</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS6900-X/T Models</td>
<td>The last 5 ports including ports on expansion slots.</td>
</tr>
<tr>
<td>OS6900-Q32</td>
<td>The last 5 ports that have a transceiver or 40G-to-10G splitter cable plugged in.</td>
</tr>
<tr>
<td>OS6900-X72</td>
<td>The last 5 ports (50-54). A port that has a 40G-to-10G splitter cable will be counted as four ports.</td>
</tr>
<tr>
<td>OS6900-V72/C32/V48C8</td>
<td>The last 5 ports. A port that has a splitter cable will be counted as four ports.</td>
</tr>
<tr>
<td>OS6900-X48C4E</td>
<td>VC not supported.</td>
</tr>
<tr>
<td>OS6860(E) Models</td>
<td>Dedicated VFL ports.</td>
</tr>
<tr>
<td>OS6860N Models</td>
<td>Dedicated VFL ports.</td>
</tr>
<tr>
<td>OS6560 Models</td>
<td>None.</td>
</tr>
<tr>
<td>OS6560 Models</td>
<td>OS6560-(P)24X4 - Ports 29-30.</td>
</tr>
<tr>
<td></td>
<td>OS6560-(P)48X4 - Ports 53-54.</td>
</tr>
<tr>
<td></td>
<td>Dedicated VFL ports. (all other models).</td>
</tr>
<tr>
<td>OS6570M Models</td>
<td>None.</td>
</tr>
<tr>
<td>OS9900</td>
<td>None. Supports static VFL ports only.</td>
</tr>
<tr>
<td>OS6465</td>
<td>OS6465-P6/P12 - None.</td>
</tr>
<tr>
<td></td>
<td>OS6465-P28 - Ports 27/28.</td>
</tr>
<tr>
<td>OS6360 Models</td>
<td>OS6360-10 port models - None.</td>
</tr>
<tr>
<td></td>
<td>OS6360-24 port models - Ports 27/28.</td>
</tr>
<tr>
<td></td>
<td>OS6360-48 port models - Ports 51/52.</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>
Usage Guidelines

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- This command is allowed only if VFL mode is auto.
- Refer to the defaults table above for information on which ports are default automatic VFL ports.
- Transceiver does not have to be present for port to be eligible as a default port.
- The OS6860N only supports a VFL link on the dedicated VFL ports.

Examples

-> virtual-chassis auto-vf-link-port 1/1/1
-> no virtual-chassis auto-vf-link-port 1/1/1

Release History

Release 7.3.4; command introduced.

Related Commands

show virtual-chassis auto-vf-link-port

MIB Objects

virtualChassisAutoVflPortTable
  virtualChassisAutoVflPortIfindex
  virtualChassisAutoVflPortRowStatus
vc-takeover

This command causes a reload of the master chassis from the running configuration in a virtual chassis environment.

vc-takeover

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The OS6900-X48C4E does not support a Virtual Chassis configuration.

- For a dual-CMM Master chassis configuration, this command triggers a local CMM takeover on the Master if both the primary and secondary CMMs are up. This will cause the secondary CMM to become the primary CMM and the NIs will remain up. The original Master chassis will remain the Master and the Slave chassis will remain the Slave.

- For a single-CMM Master chassis configuration, this command will reboot the entire Master chassis including the NIs and result in the Slave chassis becoming the Master.

Examples

-> vc-takeover
WARNING - Working Changes Will Be Lost, Confirm VC takeover (Y/N) :

Release History

Release 7.3.2; command introduced.
Related Commands

reload from

Reloads the master or slave chassis from the specified directory.

MIB Objects

N/A


**ssh-chassis**

This command allows access to the console of any chassis in a VC using the secure shell protocol (SSH).

**ssh-chassis [username@chassis-id]**

---

**Syntax Definitions**

- **username@chassis-id**: The user name and chassis ID to be accessed.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- User will be prompted to enter a password for the username being used to access the member of the VC.
- The SSH used for this feature supports only password based authentication and will not work if “SSH Enforce-Pubkey-Auth” is enabled on the switch.

**Examples**

```
-> ssh-chassis guest@2
Executing: ssh guest@127.10.2.65
(guest@127.10.2.65) Password:
```

**Release History**

Release 8.9R1; command introduced.

**Related Commands**

- **show virtual-chassis topology**: This command is used to provide a detailed status of the virtual chassis topology.

**MIB Objects**

- **N/A**
**convert configuration**

Converts an existing standalone configuration to a virtual chassis configuration.

`convert configuration to dir [reload]`

### Syntax Definitions

- **dir**  
  The name of the directory to store the virtual chassis configuration.

- **reload**  
  Reloads the switch after converting the configuration.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The OS6900-X48C4E does not support a Virtual Chassis configuration.

- This command will automatically create the new configuration files `vcsetup.cfg` and `vcboot.cfg` within the specified directory. The `vcsetup.cfg` file contains the virtual chassis manager configuration, which is specific to each individual switch. The contents of the `vcsetup.cfg` files are unique to each switch and distinct between switches. The `vcboot.cfg` file contains the generic application configuration, which is global to the entire virtual chassis topology. As a result, the `vcboot.cfg` files should have the same contents between distinct switches.

- This command will automatically copy the image files of the current running directory into the specified dir directory.

- This command is only accepted in standalone mode after a valid chassis identifier (1-6) has been configured on the switch. The command is rejected when executed in a switch already running in virtual chassis mode.

- The directory will be automatically created if it does not exist.

- The current standalone configuration files (e.g. `boot.cfg`) that may exist in the directory will remain intact. When the switches come up in virtual chassis mode following a conversion using this command, the `vcboot.cfg` files present on distinct switches may be different. However, the `vcboot.cfg` files must be the same on all switches running in virtual chassis mode. As a result, the `vcboot.cfg` file of the master will overwrite the `vcboot.cfg` file on the slave chassis and the slave will automatically reboot.
Examples

-> convert configuration to vc_dir

Release History

Release 7.3.1; command introduced.

Related Commands

show configuration snapshot  Displays the configured and operational parameters related to the virtual chassis feature on the switch.

MIB Objects

N/A
show virtual-chassis topology

This command is used to provide a detailed status of the virtual chassis topology.

show virtual-chassis [chassis-id \{oper_chassis\}] topology

Syntax Definitions

oper_chassis
The operational/current chassis ID number.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• The OS6900-X48C4E does not support a Virtual Chassis configuration.
• This command can be executed on any CMM within any switch of the system.
• When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.
• A chassis-id of 100 or 101 is used to indicate a duplicate chassis-id.

Examples

-> show virtual-chassis topology
Legend: Licenses - A: Advanced; B: Data Center

<table>
<thead>
<tr>
<th>Chas</th>
<th>Role</th>
<th>Status</th>
<th>Config</th>
<th>Chas ID</th>
<th>Pri</th>
<th>Group</th>
<th>MAC-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Master</td>
<td>Running</td>
<td>1</td>
<td>100</td>
<td>1</td>
<td>1</td>
<td>e8:e7:32:00:2a:55</td>
</tr>
<tr>
<td>2</td>
<td>Slave</td>
<td>Running</td>
<td>2</td>
<td>100</td>
<td>1</td>
<td>1</td>
<td>e8:e7:32:07:9f:e1</td>
</tr>
</tbody>
</table>

-> show virtual-chassis chassis-id 2 topology
Oper-Chassis-ID : 2,
Config-Chassis-ID : 2,
Chassis-Role : Master,
Previous-Chassis-Role : Master,
Chassis-Status : Running,
Chassis-Group : 1,
Chassis-MAC : e8:e7:32:00:2a:55,
Up-Time : 0 days 0 hours 22 minutes and 7 seconds,
Virtual Chassis Commands

show virtual-chassis topology

Designated-NI : 1,
Primary-CMM : CMM-A,
Secondary-CMM : Unknown,
Chassis-Type : OS6900,
Licence : AB,
Hello-Interval : 10,
Oper-Chassis-Priority : 100,
Config-Chassis-Priority : 100,
Oper-Control-VLAN : 4093,
Config-Control-VLAN : 4093,
VFLink Mode : static,
Number-Of-Neighbors : 5,
Number-Of-Direct-Neighbors : 3

<table>
<thead>
<tr>
<th>Chassis-ID</th>
<th>Is-Direct</th>
<th>Shortest-Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Yes</td>
<td>2/0-&gt;1/4</td>
</tr>
<tr>
<td>3</td>
<td>Yes</td>
<td>2/2-&gt;3/0</td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>2/2-&gt;3/0, 3/3-&gt;4/2</td>
</tr>
<tr>
<td>5</td>
<td>Yes</td>
<td>2/1-&gt;5/1</td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>2/0-&gt;1/4, 1/0-&gt;6/0</td>
</tr>
</tbody>
</table>

output definitions

Oper-Chassis-ID (Chas) Operational/current virtual chassis chassis identifier.
Config Chas ID The configured/next chassis identifier for the switch specified by operational chassis identifier.
Chassis-Role (Role) Chassis Role
Unassigned: Role undefined as election has not completed yet.
Master: Chassis is central point of management and control.
Slave: Chassis is an active or functional participant of the virtual chassis topology, but it is not the main entry point for management and control purposes.
Inconsis: Chassis is not an active or functional participant of the virtual chassis topology due to some inconsistent parameter, which does not match the master chassis' settings.
Startup-Err: Chassis is in start up error mode because it was unable to come up in virtual chassis mode. When a chassis assumes the Startup-Err role, its chassis status will be equal to either Invalid-Chassis-Id or Invalid-License, which are described later in this section.
Previous-Chassis-Role Previous chassis role before the last transition.
output definitions

<table>
<thead>
<tr>
<th>Chassis-Status (Status)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Init</td>
<td>Status undefined as the chassis has not completed its initialization.</td>
</tr>
<tr>
<td>Running</td>
<td>The chassis is fully operational.</td>
</tr>
<tr>
<td>Invalid-Chassis-Id</td>
<td>The chassis is not operational in virtual chassis mode because no valid chassis identifier has been found in the configuration. Typically this means that the vcsetup.cfg file is corrupted, empty or contains an invalid (e.g. out of range) chassis ID identifier.</td>
</tr>
<tr>
<td>Invalid-License</td>
<td>The chassis is not operational in virtual chassis mode because no valid advanced license has been found.</td>
</tr>
<tr>
<td>Hello-Down</td>
<td>The chassis is isolated from the rest of the virtual chassis topology participants because hello packets have not been received for a period of time greater than the hello timeout.</td>
</tr>
<tr>
<td>Duplicate-Chassis</td>
<td>This chassis is not fully operational because its operational chassis identifier matches the chassis ID of another chassis within the virtual chassis topology. As a result, a new operational chassis identifier from the range (101-102) will be allocated to this chassis.</td>
</tr>
<tr>
<td>Mis-Image</td>
<td>The chassis is not fully operational because its image versions are not consistent with the master chassis' images. In other words, the image version are not compatible and some of the software components running on this chassis are unable to interface with the software operating in the master chassis.</td>
</tr>
<tr>
<td>Mis-Chassis-Type</td>
<td>The chassis is not fully operational because its chassis type (i.e. OS6900, OS6860) is not consistent with the master chassis' type. Different chassis types cannot be mixed in the same virtual chassis topology.</td>
</tr>
<tr>
<td>Mis-Hello-Interval</td>
<td>The chassis is not fully operational because its operational hello interval is not consistent with the master chassis' operational hello interval.</td>
</tr>
<tr>
<td>Mis-Control-Vlan</td>
<td>The chassis is not fully operational because its operational control VLAN is not consistent with the master chassis' operational control VLAN.</td>
</tr>
<tr>
<td>Mis-Chassis-Group</td>
<td>The chassis is not fully operational because its chassis group does not match the master chassis' chassis group and the chassis is connected directly or indirectly to the master chassis through virtual-fabric links. This chassis is unable to join the active virtual chassis topology whose master chassis is part of.</td>
</tr>
<tr>
<td>Mis-License-Config</td>
<td>The chassis is not fully operational because its license settings do not match the master chassis' license configuration. An exact match is required to allow successful operation within the same virtual chassis topology.</td>
</tr>
<tr>
<td>Split-Topology</td>
<td>The chassis is not fully operational and all of its front panel user ports (excluding the virtual-fabric link member ports) are operationally down because a topology split has occurred. This chassis became isolated from the master chassis after all of its active virtual-fabric member ports went down or the virtual chassis manager hello timeout has expired.</td>
</tr>
<tr>
<td>Running+</td>
<td>Element added after last saved topology.</td>
</tr>
<tr>
<td>Not-Joined</td>
<td>Element missing from last saved topology.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chassis-Group (Group)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual chassis group identifier. Used to identify a group of chassis belonging to the same virtual chassis.</td>
<td></td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis-MAC (MAC-Address)</td>
<td>Chassis MAC address.</td>
</tr>
<tr>
<td>Up-Time</td>
<td>Chassis up time.</td>
</tr>
<tr>
<td>Designated-NI</td>
<td>Designated network interface module (NI), which is the module responsible for managing the inter-process communication infrastructure responsible for control communication between distinct switches within the virtual chassis topology. Only VFL capable network interface modules can be elected as designated NI. When no VFL capable network interface modules are present on a switch, the designated NI is zero (0).</td>
</tr>
<tr>
<td>Primary-CMM</td>
<td>Primary CMM slot.</td>
</tr>
<tr>
<td>Secondary-CMM</td>
<td>Secondary CMM slot.</td>
</tr>
<tr>
<td>Chassis-Type</td>
<td>The switch chassis type.</td>
</tr>
<tr>
<td>License</td>
<td>The licenses installed on the chassis.</td>
</tr>
<tr>
<td>Hello-Interval</td>
<td>The hello-interval configured for the chassis.</td>
</tr>
<tr>
<td>Oper-Chassis-Priority (Pri)</td>
<td>Operational/current chassis priority, which defines the user preference above all other election criteria, for a switch to become the master chassis of the virtual chassis topology. The greater this value the more likely a switch is to be elected as the master chassis.</td>
</tr>
<tr>
<td>Config-Chassis-Priority</td>
<td>Configured/next chassis priority, which defines the user preference above all other election criteria.</td>
</tr>
<tr>
<td>Oper-Control-VLAN</td>
<td>Operational/current virtual chassis control VLAN.</td>
</tr>
<tr>
<td>Config-Control-VLAN</td>
<td>Configured/next virtual chassis control VLAN, which will take effect after reset thereby becoming the next operational control VLAN.</td>
</tr>
<tr>
<td>Number-of-Neighbors</td>
<td>Total number of neighbor switches that are part of the active virtual chassis topology for a given chassis group.</td>
</tr>
<tr>
<td>VFLink Mode</td>
<td>The VFLink mode of the chassis: Static or Auto.</td>
</tr>
<tr>
<td>Number-of-Direct-Neighbors</td>
<td>Number of directly attached neighbor switches that are part of the active virtual chassis topology for a given chassis group These are switches directly connected to the local switch through a virtual-fabric link (VFL).</td>
</tr>
<tr>
<td>Neighbor</td>
<td>The operational chassis identifier of neighbor switch.</td>
</tr>
<tr>
<td>Is-Direct</td>
<td>Flag identifying whether a particular neighbor is directly attached to a given switch.</td>
</tr>
<tr>
<td>Shortest-Path</td>
<td>The shortest path from a given switch to a neighbor switch using the notation <code>chassis/vfl_id</code>.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command introduced.
Release 7.3.4; VFLink mode introduced.
Related Commands

- **virtual-chassis configured-chassis-id**: Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual chassis mode.

- **virtual-chassis chassis-group**: Assigns a globally unique chassis group identifier to a switch. Each peer switch in a virtual chassis domain must use the same group ID number.

- **virtual-chassis configured-chassis-priority**: Sets the configured chassis priority for a switch specified by its operational chassis identifier.

- **virtual-chassis configured-control-vlan**: Sets the configured control VLAN for a switch specified by its operational chassis identifier.

- **virtual-chassis configured-hello-interval**: Configures the virtual chassis hello interval parameter on the switch.

MIB Objects

- `virtualChassisGlobalTable`
  - `virtualChassisOperChasId`
  - `virtualChassisConfigChassisID`
  - `virtualChassisRole`
  - `virtualChassisPreviousRole`
  - `virtualChassisStatus`
  - `virtualChassisConfigPriority`
  - `virtualChassisOperPriority`
  - `virtualChassisGroup`
  - `virtualChassisMac`
  - `virtualChassisUpTime`
  - `virtualChassisDesigNI`
  - `virtualChassisPriCmm`
  - `virtualChassisSecCmm`
  - `virtualChassisOperControlVlan`
  - `virtualChassisConfigControlVlan`
  - `virtualChassisOperHelloInterval`
  - `virtualChassisConfigHelloInterval`
  - `virtualChassisType`
  - `virtualChassisLicense`
  - `virtualChassisNumOfNeighbor`
  - `virtualChassisNumOfDirectNeighbor`
show virtual-chassis consistency

This command is used to provide a detailed status of the parameters taken into account to determine the consistency of a group of switches participating in the virtual chassis topology.

show virtual-chassis [chassis-id oper_chassis] consistency

Syntax Definitions

oper_chassis

The operational/current chassis ID number.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• The OS6900-X48C4E does not support a Virtual Chassis configuration.

• This command provides a list of parameters that must be configured consistently on all switches that will participate on the virtual chassis topology to allow correct system operation.

• In order to determine the consistency of a given parameter, the switch will compare the value of such parameters on a given switch with the settings of the master chassis. Therefore consistency is always defined as a comparison with the master chassis.

• The following parameters are considered consistent if they match the settings of the master chassis: chassis type, license, chassis group, operational control VLAN, configured control VLAN, operational hello interval and configured hello interval.

• The configured chassis identifier parameter is considered consistent if it is different than the settings of the master chassis.

Examples

-> show virtual-chassis consistency
Legend: * - denotes mandatory consistency which will affect chassis status
Licenses - A: Advanced; B: Data Center

<table>
<thead>
<tr>
<th>Config</th>
<th>Oper</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chas</td>
<td>Chas</td>
<td>Chas   Hello</td>
</tr>
<tr>
<td>Chas* ID</td>
<td>Status Type*</td>
<td>Group*</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>OK</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Consistency</th>
<th>Given Chassis</th>
<th>Master Chassis</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis-ID*</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>Config-Chassis-ID</td>
<td>2</td>
<td>1</td>
<td>OK</td>
</tr>
<tr>
<td>Chassis-Type*</td>
<td>OS6900</td>
<td>OS6900</td>
<td>OK</td>
</tr>
<tr>
<td>License*</td>
<td>A</td>
<td>AB</td>
<td>NOK</td>
</tr>
<tr>
<td>Chassis-Group*</td>
<td>0</td>
<td>0</td>
<td>OK</td>
</tr>
<tr>
<td>Hello-Interval</td>
<td>10</td>
<td>10</td>
<td>OK</td>
</tr>
<tr>
<td>Oper-Control-Vlan*</td>
<td>4094</td>
<td>4094</td>
<td>OK</td>
</tr>
<tr>
<td>Config-Control-Vlan</td>
<td>4094</td>
<td>4094</td>
<td>OK</td>
</tr>
</tbody>
</table>
```

**Legend:**

- * - denotes mandatory consistency which will affect chassis status
- Licenses - A: Advanced; B: Data Center

**output definitions**

- **Chassis-ID (Chas)**: Operational/current virtual chassis chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).
- **Config-Chassis-ID (Conf Chas ID)**: The configured/next chassis identifier for the switch specified by operational chassis identifier.
- **Chassis-Type (Chas Type)**: The switch chassis type (OS6900 or OS6860).
- **License**: The licenses installed on the chassis.
- **Chassis-Group (Chas Group)**: Virtual chassis group identifier. Used to identify a group of chassis belonging to the same active virtual chassis topology.
- **Hello-Interval**: Operational/current hello-interval.
- **Oper-Control-VLAN**: Operational/current virtual chassis control VLAN.
- **Config-Control-VLAN**: Configured/next virtual chassis control VLAN, which will take effect after reset thereby becoming the next operational control VLAN.

**Status**

- **OK**: The switch is operating in virtual chassis mode and the given switch's parameter value is consistent with the settings of the master chassis.
- **NOK**: The switch is operating in virtual chassis mode and the given switch's parameter value is inconsistent with the settings of the master chassis.
- **N/A**: The switch is operating in virtual chassis mode, but the virtual chassis topology has not converged and therefore a master chassis is not yet known.
- **Disabled**: The switch is operating in standalone mode, in which there can be no virtual chassis master and hence the concept of consistency does not apply.
Release History

Release 7.3.1; command introduced.

Related Commands

- **virtual-chassis configured-chassis-id**: Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual chassis mode.
- **virtual-chassis chassis-group**: Assigns a globally unique chassis group identifier to a chassis. Each peer switch in a virtual chassis domain must use the same group ID number.
- **virtual-chassis configured-chassis-priority**: Sets the chassis priority for a chassis specified by its operational chassis identifier.
- **virtual-chassis configured-control-vlan**: Sets the configured control VLAN for a chassis specified by its operational chassis identifier.
- **virtual-chassis configured-hello-interval**: Sets the configured hello interval parameter on the switch.

MIB Objects

- **virtualChassisGlobalTable**
  - **virtualChassisOperChasId**
  - **virtualChassisConfigChassisID**
  - **virtualChassisType**
  - **virtualChassisLicense**
  - **virtualChassisGroup**
  - **virtualChassisOperControlVlan**
  - **virtualChassisConfigControlVlan**
  - **virtualChassisOperHelloInterval**
  - **virtualChassisConfigHelloInterval**
show virtual-chassis vf-link

Displays a summary of the configured and operational parameters related to the virtual fabric links on the virtual chassis topology.

show virtual-chassis [chassis-id oper_chassis] vf-link vfl_id member-port [oper_chassis/slot/port]

Syntax Definitions

oper_chassis The operational/current chassis ID number.
vfl_id The VFL identifier.
oper_chassis/slot/port The operational chassis identifier, slot, and port.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- This command can be executed on any switch within the virtual chassis topology.

Examples

-> show virtual-chassis vf-link
VFLink mode: static
Chassis/VFLink ID  Oper  Primary Port  Config Port  Active Port  Def Vlan
-------------------------------+-------+-------------+-------------+-------------+-----+
1/0  Up   1/1/3       2           2           1
2/0  Up   2/1/3       2           2           1

-> show virtual-chassis chassis-id 1 vf-link
Chassis/VFLink ID  Oper  Primary Port  Config Port  Active Port  Def Vlan
-------------------------------+-------+-------------+-------------+-------------+-----+
1/0  Up   1/1/3       2           2           1

-> show virtual-chassis vf-link member-port
Chassis/VFLink ID  Chassis/Slot/Port  Oper  Is Primary
-------------------------------+---------------+-------+---------+
1/0  1/1/1         Up   No
1/0  1/1/3         Up   Yes
2/0  2/1/3         Up   Yes
-> show virtual-chassis chassis-id 1 vf-link member-port

<table>
<thead>
<tr>
<th>Chassis/VFLink ID</th>
<th>Chassis/Slot/Port</th>
<th>Oper</th>
<th>Is Primary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/0</td>
<td>1/1/1</td>
<td>Up</td>
<td>No</td>
</tr>
<tr>
<td>1/0</td>
<td>1/1/3</td>
<td>Up</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**output definitions**

- **Chassis/VFLink ID**: Pair operational/current virtual chassis chassis identifier and virtual-fabric link (VFL) identifier.
- **Oper**: Virtual-fabric link (VFL) operational status (Up or Down).
- **Primary Port**: Primary port of the virtual-fabric link (VFL) trunk, which is the port where non-unicast packets destined a remote chassis are sent out.
- **Config Port**: Number of ports configured to operate as virtual-fabric link (VFL) member ports, i.e. ports that potentially may join a VFL.
- **Active Port**: Number of virtual-fabric link (VFL) member ports that are operational, i.e. the LACP protocol is fully operational for those ports.
- **Def Vlan**: Operational default VLAN on the virtual-fabric link (VFL).
- **Chassis/Slot/Port**: The operational chassis/slot/port tuple identifying a particular virtual-fabric link (VFL) member port.
- **Is Primary**: Indicates if this port is the primary port of the VFL.

**Release History**

- Release 7.3.1: command introduced.
- Release 7.3.4: VFLink mode introduced.

**Related Commands**

- **virtual-chassis configured-chassis-id**: Assigns a globally unique chassis identifier to the switch and enables the switch to operate in virtual chassis mode.
- **virtual-chassis vf-link create**: Configures a virtual fabric link (VFL) between two peer switches. A VFL is required to enable the Virtual Chassis operation between the two switches.
- **virtual-chassis vf-link member-port**: Configures member ports for the virtual fabric link (VFL).
- **virtual-chassis vf-link default-vlan**: Configures the default VLAN for the VFL.

**MIB Objects**

- `virtualChassisLinkTable`
- `virtualChassisOperChasID`
- `virtualChassisLinkOperDefaultVlan`
- `virtualChassisLinkLinkOperStatus`
- `virtualChassisLinkPrimaryPort`
- `virtualChassisLinkConfigPortNum`
- `virtualChassisLinkActivePortNum`
- `virtualChassisLinkId`
- `virtualChassisVflMemberPortIfindex`
- `virtualChassisVflMemberPortRowStatus`
show virtual-chassis auto-vf-link-port

Displays a summary of the auto VFL ports.

**show virtual-chassis [chassis-id oper_chassis] auto-vf-link-port [chassis/slot/port]**

---

**Syntax Definitions**

- `oper_chassis`: The operational/current chassis ID number.
- `oper_chassis/slot/port`: The operational chassis identifier, slot, and port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platforms</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- This command can be executed on any switch within the virtual chassis topology.

**Examples**

```
-> show virtual-chassis auto-vf-link-port
Chassis/Slot/Port VFL ID VFL member status
-------------------------------+----------------+-----------------------
 1/1/1                      1/0                          Down
 1/1/3                      1/1                          Up
```

**output definitions**

- **Chassis/Slot/Port**: The chassis/slot/port identifier.
- **VFL ID**: The VFL identifier.
- **VFL member status**: The status of the VFL member port. Up or Down.

**Release History**

Release 7.3.4; command introduced.
Related Commands

`virtual-chassis auto-vf-link-port` Configures the port to be an automatic VFL port.

MIB Objects

`virtualChassisLinkTable`
  `virtualChassisOperChasID`
  `virtualChassisVflMemberPortRowStatus`
**show virtual-chassis chassis-reset-list**

This command displays the list of all chassis that must be reset along with a specified chassis in order to prevent a virtual chassis topology split.

**show virtual-chassis [chassis-id `oper_chassis`] chassis-reset-list**

---

**Syntax Definitions**

- `oper_chassis` The operational/current chassis ID number.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.

---

**Examples**

````
-> show virtual-chassis chassis-reset-list
Chas  Chassis reset list
--------+---------------------
  1     1
  2     2

-> show virtual-chassis chassis-id 1 chassis-reset-list
Chas  Chassis reset list
--------+---------------------
  1     1
```

---

**output definitions**

- **Chas** Operational/current virtual chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).
- **Chassis reset list** A list of operational chassis identifiers, which define which switches must be reset, along with the switch given by Chas in order to prevent a split of the virtual chassis topology.
Release History

Release 7.3.1; command introduced.

Related Commands

show virtual-chassis topology  Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology

MIB Objects

virtualChassisChassisResetListTable
  virtualChassisOperChasId
  virtualChassisChassisResetList
**show virtual-chassis slot-reset-list**

For a given chassis and network interface module (NI), displays status information specifying whether bringing down or extracting such NI will lead to a virtual chassis topology split.

```
show virtual-chassis [chassis-id oper_chassis] slot-reset-list
```

**Syntax Definitions**

`oper_chassis` 
The operational/current chassis ID number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.
- On the OmniSwitch 6900, the slot number depicted in this command always refers to the main board of the switch (i.e. slot number 1). In other words, this command does not present the status related to expansion boards.

**Examples**

```
-> show virtual-chassis slot-reset-list
Chas  Slot  Reset status
---------+---------+--------------
  1      1      Split
  2      1      Split

-> show virtual-chassis chassis-id 1 slot-reset-list
Chas  Slot  Reset status
---------+---------+--------------
  1      1      Split
```
### output definitions

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chas</strong></td>
<td>Operational/current virtual chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).</td>
</tr>
<tr>
<td><strong>Slot</strong></td>
<td>Slot number identifying a particular network interface module (NI). For OmniSwitch 6900 switches, the slot number is always equal to 1.</td>
</tr>
</tbody>
</table>
| **Reset Status** | For the network interface module (NI) identified by the pair (Chas, Slot), this command displays status information specifying whether bringing down or extracting such network interface module (NI) will lead to a virtual chassis topology split according to the following definitions.  
**Supported**: The network interface module can be reset without splitting the virtual chassis topology.  
**Split**: Resetting this network interface module will cause a virtual chassis topology split. |

### Release History

Release 7.3.1; command introduced.

### Related Commands

**show virtual-chassis topology** Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

### MIB Objects

- virtualChassisSlotResetStatusTable
- virtualChassisOperChasID
- virtualChassisSlotResetStatus
**show virtual-chassis neighbors**

This command displays a list of which neighbors are connected via which VFL for a virtual chassis.

```
show virtual-chassis [chassis-id oper_chassis] neighbors
```

**Syntax Definitions**

- `oper_chassis` The operational/current chassis ID number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>VFL VFL VFL VFL VFL</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- When no operational chassis identifier is specified the command will show data related to the entire virtual chassis system.

**Examples**

```
-> show virtual-chassis neighbors
Chas VFL VFL VFL VFL VFL
ID 0 1 2 3 4
-----+---+---+---+---+---
1 2 3 4 5 6
2 1 3 4 5 6
3 1 2 4 5 6
4 1 2 3 5 6
5 1 2 3 4 6
6 1 2 3 4 5

-> show virtual-chassis chassis-id 2 neighbors
Chas VFL VFL VFL VFL VFL
ID 0 1 2 3 4
-----+---+---+---+---+---
2 1 3 4 5 6
```
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chas ID</td>
<td>Operational/current virtual chassis identifier. The operational chassis identifier when a switch operates in standalone mode is zero (0).</td>
</tr>
<tr>
<td>VFL</td>
<td>The VLF identifier connecting to the remote chassis listed in the table.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command introduced.

Related Commands

**show virtual-chassis topology**

Displays details about the configured and operational parameters related to all switches participating in the virtual chassis topology.

MIB Objects

- virtualChassisVflTable
  - virtualChassisOperChasID
  - virtualChassisVflId
  - virtualChassisVflDirectNeighborChasId
show configuration vcm-snapshot chassis-id

Displays a snapshot of the switch specific virtual chassis configuration for a switch running in virtual chassis mode.

**show configuration vcm-snapshot chassis-id oper_chassis**

---

### Syntax Definitions

*oper_chassis*  
The operational/current chassis ID number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- When a switch operates in standalone mode, this command is not supported. In this case, we must use the `show configuration snapshot virtual chassis` to obtain a snapshot of the switch specific virtual chassis configuration.

### Examples

```
-> show configuration vcm-snapshot chassis-id 1
! Virtual Chassis Manager:
  virtual-chassis chassis-id 1 configured-chassis-id 1
  virtual-chassis chassis-id 1 vf-link 0 create
  virtual-chassis chassis-id 1 vf-link 0 member-port 1/8/1
  virtual-chassis chassis-id 1 configured-control-vlan 4091
  virtual-chassis chassis-id 1 chassis-group 1

! IP:
  ip interface local chassis-id 1 emp address 10.255.76.21 mask 255.255.255.0
```

### Release History

Release 7.3.1; command introduced.
Virtual Chassis Commands

show configuration vcm-snapshot chassis-id

Related Commands

**show configuration snapshot**  Displays the configured and operational parameters related to the virtual chassis feature on the switch.

MIB Objects

N/A
virtual-chassis split-protection admin-state

Enable or disables the VC split protection feature.

virtual-chassis split-protection admin-state {enable | disable}

Syntax Definitions

**enable**
Enables VC split protection.

**disable**
Disables VC split protection.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- VCSP cannot be enabled before assigning a link aggregate.
- VCSP and the helper functionality can be enabled on the same link aggregate.
- The virtual chassis and its helper cannot have the same Group ID.

Examples

- `virtual-chassis split-protection admin-state enable`
- `virtual-chassis split-protection admin-state disable`

Release History

Release 7.3.4.R02; command was introduced.
Related Commands

- **show virtual-chassis split-protection status**
  Displays all the information related to VCSP when enabled.

- **virtual-chassis split-protection linkagg**
  Assigns a link aggregate for use with VCSP.

MIB Objects

- `alaVCSPConfigInfo`
- `alaVCSPAdminState`
**virtual-chassis split-protection linkagg**

Assigns a link aggregate for use with VCSP.

```
virtual-chassis split-protection linkagg agg_id
```

```
no virtual-chassis split-protection linkagg
```

**Syntax Definitions**

```
agg_id
```
The link aggregate ID number to associate with the helper for VCSP support. The valid range is 0–255.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- Use the `no` form of this command to remove the link aggregate assignment.
- This command must be used to configure VC split protection `linkagg` before enabling VC split protection.

**Examples**

```
-> virtual-chassis split-protection linkagg 1
```

**Release History**

Release 7.3.4.R02; command was introduced.
Related Commands

show virtual-chassis split-protection status  
Displays all the information related to VCSP when enabled.

MIB Objects

alaVCSPConfigInfo
  alaVCSPLinkaggID
virtual-chassis split-protection guard-timer

Configures the timer value for how long the master will wait to receive VCSP PDUs before beginning transmission of VCSP PDUs.

virtual-chassis split-protection guard-timer \texttt{time}

\textbf{Syntax Definitions}

\texttt{time} \hspace{2cm} Time interval to wait on boot up before choosing any state. The valid range is 30–100 seconds.

\textbf{Defaults}

\begin{tabular}{|c|c|}
\hline
\texttt{parameter} & \texttt{default} \\
\hline
\texttt{time} & 30 seconds \\
\hline
\end{tabular}

\textbf{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

\begin{tabular}{|c|c|c|c|c|c|c|c|c|c|}
\hline
\hline
Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes \\
\hline
\end{tabular}

\textbf{Usage Guidelines}

\begin{itemize}
\item The OS6900-X48C4E does not support a Virtual Chassis configuration.
\item Changes to the Guard timer only take affect after reboot or by disabling and re-enabling VC split protection.
\end{itemize}

\textbf{Examples}

\texttt{\rightarrow virtual-chassis split-protection guard-timer 60}

\textbf{Release History}

Release 7.3.4.R02; command was introduced.
Related Commands

```
show virtual-chassis split-protection status
```
Displays all the information related to VCSP when enabled.

MIB Objects

```
alaVCSPConfigInfo
  alaVCSPGuardTimer
```
**virtual-chassis split-protection helper admin-state**

Enables or disables the helper functionality on the helper device.

```bash
virtual-chassis split-protection helper admin-state {enable | disable}
```

**Syntax Definitions**

- `enable` Enables VC split protection helper functionality.
- `disable` Disables VC split protection helper functionality.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- Use this command on the helper device to enable the helper functionality.
- The helper functionality can be enabled on a device that is running VCSP.
- The virtual chassis and its helper cannot have the same Group ID.

**Examples**

```bash
-> virtual-chassis split-protection helper admin-state enable
-> virtual-chassis split-protection helper admin-state disable
```

**Release History**

Release 7.3.4.R02; command was introduced.
Related Commands

```
virtual-chassis split-protection helper admin-state
```

Configures the link aggregate on which to apply the VCSP protocol for the helper device.

MIB Objects

```
alaVCSPHelperGlobalConfig
alaVCSPHelperAdminState
```
**virtual-chassis split-protection helper linkagg**

Configures the link aggregate ID on which to apply the VCSP protocol on the helper device.

```bash
virtual-chassis split-protection helper linkagg agg_id

no virtual-chassis split-protection helper linkagg
```

**Syntax Definitions**

`agg_id` The link aggregate ID number to associate with the helper for VCSP support. The valid range is 0–255.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OS6900-X48C4E does not support a Virtual Chassis configuration.
- Use the `no` form of this command to remove the link aggregate assignment.
- Use this command on the helper device to enable the VCSP protocol on the helper link aggregate.

**Examples**

-> `virtual-chassis split-protection helper linkagg 1`

-> `no virtual-chassis split-protection helper linkagg`

**Release History**

Release 7.3.4.R02; command was introduced.
Related Commands

- **show virtual-chassis split-protection status**
  Displays the VCSP Helper status of the Link Aggregation ID assigned.

- **virtual-chassis split-protection helper admin-state**
  Enables or disables to helper functionality.

MIB Objects

- **alaVCSPHelperLinkaggTable**
  - **alaVCSPHelperLinkaggId**
  - **alaVCSPHelperLinkaggRowStatus**
**show virtual-chassis split-protection status**

Displays all the information related to VCSP when enabled.

**show virtual-chassis split-protection status**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The OS6900-X48C4E does not support a Virtual Chassis configuration.

**Examples**

-> show virtual-chassis split-protection status

VCSP admin status: enabled
VCSP operational status: Active
VCSP linkagg: 31
VCSP Guard Timer: 30
VCSP Uptime: 00d:00h:00m:00s,
VCSP Protection Uptime: 00d:00h:00m:00s

**Release History**

Release 7.3.4.R02; command was introduced.

**Related Commands**

`virtual-chassis split-protection admin-state` Enable or disables the VC split protection feature.
MIB Objects

alaVCSPConfigInfo
  alaVCSPAdminState
  alaVCSPOperState
  alaVCSPLinkaggId
  alaVCSPGuardTimer
  alaVCSPUptime
  alaVCSPProtectionStateUptime
### show virtual-chassis split-protection vc-units

Displays the VCSP state of all VC units.

#### Syntax Definitions

N/A

#### Defaults

N/A

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The OS6900-X48C4E does not support a Virtual Chassis configuration.

#### Examples

```bash
-> show virtual-chassis split-protection vc-units

CHASSIS    STATE
----------+---------
   1       ACTIVE
   2       ACTIVE
```

#### Release History

Release 7.3.4.R02; command was introduced.

#### Related Commands

- **virtual-chassis split-protection admin-state**: Enable or disables the VC split protection feature.

#### MIB Objects

- `alaVCSPStateTable`
- `alaVCSPTableSlotNiNumber`
- `alaVCSPTableOperState`
**show virtual-chassis split-protection helper status**

Displays the VCSP Helper status of the assigned link aggregation ID.

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The OS6900-X48C4E does not support a Virtual Chassis configuration.

### Examples

```
-> show virtual-chassis split-protection helper status
VC Split-Protection Helper Status : Enabled
    Link Aggregation Id       VC Split-Protection Status
-------------------------+----------------------------------------------------
            3                Enabled
```

### Release History

Release 7.3.4.R02; command was introduced.

### Related Commands

- **virtual-chassis split-protection admin-state**
  
  Enable or disables the VC split protection feature.

### MIB Objects

- alaVCSFStateTable
  - alaVCSPTableSlotNiNumber
  - alaVCSPTableOperState
Virtual Chassis Commands

show virtual-chassis split-protection helper status
14  Ethernet Ring Protection Commands

Ethernet Ring Protection (ERP) is a protection switching mechanism for Ethernet ring topologies, such as multi-ring and ladder networks. The implementation of ERP on the OmniSwitch is based on ERP Version 2 (ITU-T G.8032/Y.1344 to 2010) using the Ring Automatic Protection Switching (R-APS) protocol to coordinate and prevent network loops within a bridged Ethernet ring.

ERPv2 supports multi-rings and ladder to ladder networks. ERPv2 functionalities allow configuration of Sub-Rings within a Master Ethernet Ring, interconnected nodes and shared links between the rings.

MIB information for Ethernet Ring Protection commands is as follows:

Filename:  ALCATEL-IND1-ERP-MIB.mib
Module:    alcatelIND1ERPMIB

A summary of available commands is listed here:

```
  erp-ring
  erp-ring rpl-node
  erp-ring wait-to-restore
  erp-ring enable
  erp-ring guard-timer
  erp-ring sub-ring
  erp-ring virtual-channel
  erp-ring revertive
  erp-ring clear
  erp-ring ethoam-event
  erp-ring sap-neighbor
  clear erp statistics
  show erp
  show erp statistics
```
**erp-ring**

Creates an Ethernet Ring Protection (ERP) using the specified ports and service VLAN ID. The service VLAN transmits ERP control traffic, such as Ring Automatic Protection Switching (R-APS) messages, through the ring. The specified level number identifies an APS Management Entity Group (MEG) to which the service VLAN belongs.

```
```

**Syntax Definitions**

- `ring_id`: The ERP ring ID number. The valid range is 1 to 2147483647.
- `chassis`: The chassis identifier.
- `slot/port`: The slot number for the module and the physical port number on that module.
- `agg_id`: The link aggregate ID number.
- `access-[tagged | untagged]`: Specifies the ERP Control (Service) VLAN mapping to tagged or untagged port or linkagg on the access port1 or port 2.
  - If the ERP control VLAN is mapped to tagged SAP, then configure ERP ring as access-tagged.
  - If the ERP control VLAN is mapped to untagged SAP, configure the ERP ring as access-untagged.
  
  *This parameter is supported only on the OmniSwitch 9900, OmniSwitch 6900, OmniSwitch 6860, and OmniSwitch 6860N.*

- `mac_address`: MAC address of the remote system of the BEB where the other end of the ERP ring is connected as the access port.
  
  Only either of port2 or remote system can be configured.

  *This parameter is supported only on the OmniSwitch 9900, OmniSwitch 6900, OmniSwitch 6860, and OmniSwitch 6860N.*

- `vlan_id`: The service VLAN ID number. The valid range is 1 to 4094.
- `level`: The MEG level number for the service VLAN. The valid range is 0 to 7.
- `guard-timer`: The guard timer value, in centi seconds, for the ring node.
- `wrt-timer`: The wait-to-restore timer value, in minutes, for the Ring Protection Link (RPL) node.
- `enable`: Administratively enables the ERP ring.
- `disable`: Administratively disables the ERP ring.
Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>guard_timer</td>
<td>50</td>
</tr>
<tr>
<td>wtr_timer</td>
<td>5</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove a ring from the switch configuration. Administratively disable the ring ports before deleting the ring to avoid creating any network loops. Once the ring is deleted, ensure that the same ports are administratively enabled under Spanning Tree control.

- The specified ring identification number must be unique within a switch.

- ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.

- BEB cannot be a RPL node. Hence, RPL port shall not be configured on SPB network. The RPL port cannot be configured as a SAP neighbor.

- Each ERP ring can have only two access port connections into the underlay network.

- For the SPB service associated with the ERP service VLAN, it has to be configured in the Control bridge VLAN (BVLAN) of the SPB network. This will ensure reachability to all nodes of the SPB network.

- In case where the underlay network needs to support more than one ERP ring, then
  - Ensure there is no overlap in the VLAN range supported within the ERP rings. That is, each ERP ring must have an exclusive range of VLANs including the service VLAN relative to the other ERP rings.
  - In the underlay network, the services association with the ERP VLANS is exclusive to each ring. That is, the service IDs (for example, ISID, VNID) cannot extend across/into the other ERP rings.

- If a port is tagged with the service VLAN ID or the service VLAN is the default VLAN for the port, then the port is not eligible to become an ERP ring port.

- Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.
- If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.

- Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.

- The service VLAN can belong to only one ERP ring at a time. A maximum of 64 rings are allowed per switch.

- The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.

- An ERP ring port can belong to only one ERP ring at a time.

- Create an ERP type NNI-SVLAN binding before establishing an ERP ring on that SVLAN-NNI binding.

**Examples**

```
-> erp-ring 1 port1 1/1/1 port2 2/4/1 service-vlan 10 level 2 enable
-> erp-ring 2 port1 linkagg 1 port2 2/10/1 service-vlan 20 level 2
-> erp-ring 3 port1 linkagg 2 port2 linkagg 4 service-vlan 30 level 7
-> no erp-ring 2
-> erp-ring 1 port1 access-tagged 1/1/1 port2 access-tagged 1/1/2 service-vlan 10 level 1
-> erp-ring 1 port1 access-untagged 1/1/1 port2 access-untagged 1/1/2 service-vlan 10 level 1
-> erp-ring 1 port1 access-untagged 1/1/1 spb remote-system 00:11:22:33:44:55 service-vlan 100 level 1
-> erp-ring 1 port1 access-untagged linkagg 1 spb remote-system 00:11:22:33:44:55 service-vlan 100 level 1
-> no erp-ring 2
```

**Release History**

Release 7.1.1; command introduced.
Release 8.8R1; **access-[tagged | untagged]**, **spb-remote-system** keywords introduced.

**Related Commands**

- **show erp** Displays the ERP ring configuration for the switch.
- **show erp statistics** Displays ERP ring statistics.
- **ethernet-service svlan nni** Creates an NNI-SVLAN binding.

**MIB Objects**

- **alaErpRingServiceVid**
- **alaErpRingMEGLevel**
- **alaErpRingStatus**
- **alaErpRingPort1**
- **alaErpRingPort2**
- **alaErpRingWaitToRestore**
- **alaErpRingGuardTimer**
alaErpRingRowStatus
alaErpRingRowStatus
alaErpRingSpbRemoteId
alaErpRingPort1ServiceVlanTagStatus
alaErpRingPort2ServiceVlanTagStatus
**erp-ring rpl-node**

Configures a switch as a Ring Protection Link (RPL) node. This command also identifies the ERP port as an RPL connection port. The RPL remains blocked to prevent loops within the ERP ring.

```
erp-ring ring_id rpl-node {port chassis/slot/port | linkagg agg_id}
no erp-ring ring_id rpl-node
```

**Syntax Definitions**

- **ring_id**
  An existing ERP ring ID number. The valid range is 1 to 2147483647.
- **chassis**
  The chassis identifier.
- **slot/port**
  The slot number for the module and the physical port number on that module.
- **agg_id**
  The link aggregate ID number.

**Defaults**

NA

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the RPL designation for the specified ring.
- The RPL node can be configured only when the ring is disabled. RPL configuration applied to the Ethernet ring while it is enabled is rejected.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only to ERP ring ports; ports not configured as ERP ring ports are not eligible to become RPL ports.
- Only one of the two ring ports configured for the switch can be designated as an RPL node port.

**Examples**

```
-> erp-ring 1 rpl-node port 2/1
-> erp-ring 2 rpl-node linkagg 2
-> no erp-ring 2 rpl-node
```
**Release History**
Release 7.1.1; command introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>erp-ring</code></td>
<td>Configures an ERP ring.</td>
</tr>
<tr>
<td><code>erp-ring wait-to-restore</code></td>
<td>Configures the wait-to-restore timer value for the Ring Protection Link (RPL) node.</td>
</tr>
<tr>
<td><code>show erp</code></td>
<td>Displays the ERP ring configuration for the switch.</td>
</tr>
</tbody>
</table>

**MIB Objects**

alaErpRingPortEntry
- alaErpRingPortIfIndex
- alaErpRingPortType
**erp-ring wait-to-restore**

Configures the wait-to-restore timer value for the Ring Protection Link (RPL) switch. This timer determines the number of minutes the RPL switch waits before returning the RPL ports to a blocked state after the ERP ring has recovered from a link failure.

**Syntax**

```
erp-ring ring_id wait-to-restore wtr_timer
```

**no erp-ring ring_id wait-to-restore**

**Syntax Definitions**

- **ring_id**
  - An existing ERP ring ID number. The valid range is 1 to 2147483647.

- **wtr_timer**
  - The number of minutes to wait before restoring the RPL to a blocked state. The valid range is 1 to 12.

**Defaults**

By default, the wait-to-restore timer value is set to 5 minutes.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to set the timer back to the default setting of 5 minutes.
- The specified ERP ring ID must exist in the switch configuration.
- This command applies only on a switch that serves as the RPL node for the ERP ring.

**Examples**

```
-> erp-ring 1 wait-to-restore 6
-> no erp-ring 1 wait-to-restore
```

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- **erp-ring**
  - Configures an ERP ring.

- **erp-ring rpl-node**
  - Configures a Ring Protection Link (RPL) port connection.

- **show erp**
  - Displays the ERP ring configuration for the switch.

**MIB Objects**

- **alaErpRingId**
- **alaErpRingWaitToRestoreTimer**
**erp-ring enable**

Enables or disables an ERP ring identified by the specified ring ID. This command applies to enabling or disabling existing ERP rings.

```
erp-ring ring_id {enable | disable}
```

### Syntax Definitions

- **ring_id**
  
  An existing ERP ring ID number. The valid range is 1 to 2147483647.

- **enable**
  
  Enables the specified ring ID.

- **disable**
  
  Disables the specified ring ID.

### Defaults

By default, ERP rings are disabled when they are created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The specified ring ID must exist in the switch configuration.
- Enabling a ring is also allowed at the time the ring is created.

### Examples

```
-> erp-ring 1 enable
-> erp-ring 1 disable
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- **erp-ring**
  - Configures an ERP ring.
- **show erp**
  - Displays the ERP ring configuration for the switch.

**MIB Objects**

- **alaErpRingId**
- **alaErpRingStatus**
**erp-ring guard-timer**

Configures the guard timer value for the specified ERP ring node. The guard timer is used to prevent ring nodes from receiving outdated Ring Automatic Protection Switching (R-APS) messages. During the amount of time determined by this timer, all received R-APS messages are ignored by the ring protection control process.

```
erp-ring ring_id guard-timer guard_timer
no erp-ring ring_id guard-timer
```

**Syntax Definitions**

- **ring_id**: An existing ERP ring ID number. The valid range is 1 to 2147483647.
- **guard_timer**: The guard timer value. The valid range is 1–200 centi-secs.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>guard_timer</td>
<td>50</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to set the timer back to the default value of 50 centi-secs.
- The specified ring ID must exist in the switch configuration.

**Examples**

```
-> erp-ring 1 guard-timer 10
-> no erp-ring 1 guard-timer
```

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- **erp-ring**
  Configures an ERP ring.

- **show erp**
  Displays the ERP ring configuration for the switch.

**MIB Objects**

- **alaErpRingId**
  - **alaErpRingGuardTimer**
**erp-ring sub-ring**

Creates an Ethernet Ring Protection (ERP) sub-ring.

```
erp-ring ring_id sub-ring-port {chassis/slot/port | linkagg agg_id} service-vlan vlan_id level level_num [guard-timer guard_timer] [wait-to-restore-timer wtr_timer] [enable | disable]
```

**Syntax Definitions**

- `ring_id`: The ERP ring ID number. The valid range is 1 to 2147483647.
- `chassis`: The chassis identifier.
- `slot/port`: The slot number for the module and the physical port number on that module.
- `agg_id`: The link aggregate ID number.
- `vlan_id`: The service VLAN ID number. The valid range is 1 to 4094.
- `level_num`: The MEG level number for the service VLAN. The valid range is 0 to 7.
- `guard_timer`: The guard timer value, in centi-secs, for the ring node.
- `wtr_timer`: The wait-to-restore timer value, in minutes, for the Ring Protection Link (RPL) node.
- `enable`: Administratively enables the ERP sub-ring.
- `disable`: Administratively disables the ERP sub-ring.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>guard_timer</td>
<td>50</td>
</tr>
<tr>
<td>wtr_timer</td>
<td>5</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a sub-ring from the switch configuration.
- Administratively disable ring ports before deleting the ring to avoid creating any network loops. Once the ring is deleted, ensure that the same ports are administratively enabled under Spanning Tree control.
The specified ring identification number must be unique within a switch.

ERP is not supported on mobile ports, mirroring ports, link aggregate member ports, high availability ports, Multicast VLAN receiver ports (ERP is supported on Multicast VLAN sender ports only), VLAN Stacking user network interface (UNI) ports, or RRSTP ring ports.

If a port is tagged with the service VLAN ID or the service VLAN is the default VLAN for the port, the port is not eligible to become an ERP ring port.

Specify an existing VLAN ID for the service VLAN ID. Use the same VLAN ID and level number for the service VLAN on each switch that participates in the ERP ring.

If the ERP switch participates in an Ethernet OAM Maintenance Domain (MD), configure the ERP service VLAN to use the same level number that is used for the Ethernet OAM MD.

Specify a static VLAN ID for the ERP service VLAN; dynamic VLANs are not configurable as service VLANs.

The service VLAN can belong to only one ERP ring at a time. A maximum of four rings are allowed per switch.

The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-ERP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.

An ERP ring port can belong to only one ERP ring at a time.

An ERP type NNI-SVLAN binding must be created before establishing an ERP ring on that SVLAN-NNI binding.

Examples

- `-> erp-ring 1 sub-ring-port 1/1 service-vlan 10 level 2 enable`
- `-> erp-ring 2 sub-ring-port linkagg 1 port2 2/10 service-vlan 20 level 2`
- `-> no erp-ring 2`

Release History

Release 7.3.1; command introduced.

Related Commands

- `erp-ring` Creates an Ethernet Ring Protection (ERP) ring.
- `show erp` Displays the ERP ring configuration for the switch.
- `show erp statistics` Displays ERP ring statistics.
- `ethernet-service svlan nni` Creates a NNI-SVLAN binding.
### MIB Objects

- alaErpRingTable
- alaErpRingId
- alaErpRingServiceVid
- alaErpRingMEGLevel
- alaErpRingStatus
- alaErpRingPort1
- alaErpRingPort2
- alaErpRingWaitToRestore
- alaErpRingGuardTimer
- alaErpRingRowStatus
**erp-ring virtual-channel**

Enables or disables an Ethernet Ring Protection (ERP) Ring Virtual Channel.

`erp-ring ring_id virtual-channel [enable | disable]`

---

**Syntax Definitions**

- **ring_id**
  - The ERP ring ID number. The valid range is 1 to 2147483647.

- **enable**
  - Administratively enables the ERP virtual channel. If enabled, Ring Automatic Protection Switching (R-APS) protocol messages are encapsulated and transmitted over a virtual channel configured on the major ring.

- **disable**
  - Administratively disables the ERP virtual channel. If disabled, R-APS messages are terminated at the interconnection nodes between the rings but not blocked at the Ring Protection Link (RPL) of the sub-ring.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The specified ring identification number must be unique within a switch.
- The ring identified by Ring ID must be created before configuring the virtual channel state for ring node.

---

**Examples**

`-> erp-ring 2 virtual-channel disable`  
`-> erp-ring 1 virtual-channel enable`

---

**Release History**

Release 7.3.1; command introduced.
**Related Commands**

- **erp-ring**
  Creates an Ethernet Ring Protection (ERP) ring.

- **erp-ring sub-ring**
  Creates an Ethernet Ring Protection (ERP) ring sub ring.

- **show erp**
  Displays the ERP ring configuration for the switch.

- **show erp statistics**
  Displays ERP ring statistics.

**MIB Objects**

- alaErpRingTable
  - alaErpRingId
  - alaErpRingVirtualChannel
erp-ring revertive

Enables or disables revertive mode on the specified node.

\texttt{erp-ring} \textit{ring\_id} revertive \{enable | disable\}

\textbf{Syntax Definitions}

- \textit{ring\_id} \quad The ERP ring ID number. The valid range is 1 to 2147483647.
- \textit{enable} \quad Administratively enables Revertive Mode. Now, if the RPL is unblocked due to a failure within the ring, the RPL automatically reverts to the “Blocked” state when the failed link recovers.
- \textit{disable} \quad Administratively disables Revertive Mode. Now, If the RPL is unblocked due to a failure within the ring, the RPL does not automatically revert to “Blocked” state when the failed link recovers.

\textbf{Defaults}

\begin{tabular}{ll}
\hline
parameter & default \\
\hline
\texttt{enable | disable} & \texttt{enable} \\
\hline
\end{tabular}

\textbf{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

\begin{tabular}{|c|c|c|c|c|c|c|c|c|c|}
\hline
\hline
No & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes \\
\hline
\end{tabular}

\textbf{Usage Guidelines}

- The specified ring identification number must be unique within a switch.
- The ring identified by the Ring ID must be created using the \texttt{erp-ring} command, before configuring the revertive mode for ring node.

\textbf{Examples}

\begin{verbatim}
-> erp-ring 1 revertive enable
-> erp-ring 2 revertive disable
\end{verbatim}

\textbf{Release History}

Release 7.3.1; command introduced.
**Related Commands**

- **erp-ring**: Creates an Ethernet Ring Protection (ERP) ring.
- **erp-ring sub-ring**: Creates an Ethernet Ring Protection (ERP) ring sub ring.
- **erp-ring clear**: Clears any pending state (for example, non-revertive restoring).
- **show erp**: Displays the ERP ring configuration for the switch.
- **show erp statistics**: Displays ERP ring statistics.

**MIB Objects**

- **alaErpRingTable**
  - **alaErpRingId**
  - **alaErpRingRevertive**
**erp-ring clear**

Clears any pending state (for example, non-revertive restoring).

**erp-ring ring_id clear**

---

### Syntax Definitions

<table>
<thead>
<tr>
<th>ring_id</th>
<th>The ERP ring ID number. The valid range is 1 to 2147483647.</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Clears any pending state on the ring.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The specified ring identification number must be unique within a switch.

### Examples

```
-> erp-ring 1 clear
```

### Release History

Release 7.3.1; command introduced.
Related Commands

**erp-ring**
- Creates an Ethernet Ring Protection (ERP) ring.

**erp-ring sub-ring**
- Creates an Ethernet Ring Protection (ERP) ring sub ring.

**show erp**
- Displays the ERP ring configuration for the switch.

**show erp statistics**
- Displays ERP ring statistics.

MIB Objects

alaErpRingTable
  - alaErpRingId
  - alaErpRingClearAction
**erp-ring ethoam-event**

Configures a ring port to accept a “loss of connectivity” event from Ethernet OAM for a remote endpoint.

```
erp-ring ring_id ethoam-event {chassis/slot/port | linkagg agg_id} remote-endpoint mep_id
```

```
no erp-ring ring_id ethoam-event {chassis/slot/port | linkagg agg_id}
```

### Syntax Definitions

- `ring_id`: The ERP ring ID number. The valid range is 1 to 2147483647.
- `chassis`: The chassis identifier.
- `slot/port`: The slot number for the module and the physical port number on that module.
- `agg_id`: The link aggregate ID number.
- `mep_id`: The remote endpoint ID.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The specified ring identification number must be unique within a switch.

### Examples

- `-> erp-ring 1 ethoam-event 1/1 remote-endpoint 10`
- `-> erp-ring 1 ethoam-event linkagg 1 remote-endpoint 10`

### Release History

Release 7.3.1; command introduced.
**Related Commands**

- `erp-ring` Creates an Ethernet Ring Protection (ERP) ring.
- `erp-ring sub-ring` Creates an Ethernet Ring Protection (ERP) ring sub ring.
- `show erp` Displays the ERP ring configuration for the switch.
- `show erp statistics` Displays ERP ring statistics.

**MIB Objects**

alaErpRingTable
  - alaErpRingId
  - alaErpRingPortIfIndex
  - alaErpRingPortEthOAMEvent
  - alaErpRingPortRmepId
**erp-ring sap-neighbor**

Configures an ERP ring SAP neighbor. The SAP neighbor port is on the ERP ring node, which has the connection to the BEB's SAP port.

```
erp-ring  ring_id sap-neighbor {port chassis/slot/port | linkagg agg_id}
```

```
no erp-ring  ring_id sap-neighbor {port chassis/slot/port | linkagg agg_id}
```

### Syntax Definitions

- **ring_id**
  - The ERP ring ID number. The valid range is 1 to 2147483647.

- **chassis**
  - The chassis identifier.

- **slot/port**
  - The slot number for the module and the physical port number on that module.

- **agg_id**
  - The link aggregate ID number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The SAP neighbor port cannot be configured as the RPL port.

### Examples

```
-> erp-ring 10 sap-neighbor port 1/1/2
```

### Release History

Release 8.8R1; command introduced.
Related Commands

**erp-ring**
Creates an Ethernet Ring Protection (ERP) ring.

**show erp**
Displays the ERP ring configuration for the switch.

**MIB Objects**

alaErpRingPortTable
alaErpRingId
alaErpRingPortIfIndex
alaErpRingPortIsSAPNeighbor
clear erp statistics

Clears ERP statistics for all rings, a specific ring, or a specific ring port.

```
clear erp statistics [ring ring_id [port chassis/slot/port | linkagg agg_id]]
```

### Syntax Definitions

- **ring_id**: An existing ERP ring ID number. The valid range is 1 to 2147483647.
- **chassis**: The chassis identifier.
- **slot/port**: The slot number for the module and the physical port number on that module.
- **agg_id**: The link aggregate ID number.

### Defaults

By default, statistics are cleared for all ERP rings in the switch configuration.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a ring ID to clear the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to clear the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

### Examples

```
-> clear erp statistics
-> clear erp statistics ring 5
-> clear erp statistics ring 5 port 1/2
-> clear erp statistics ring 5 linkagg 10
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- **erp-ring**
  - Configures an ERP ring.

- **show erp**
  - Displays the ERP ring configuration for the switch.

- **show erp statistics**
  - Displays ERP ring statistics.

**MIB Objects**

- `alaErpClearStats`
- `alaErpRingTable`
  - `alaErpRingId`
  - `alaErpRingClearStats`
- `alaErpRingPortTable`
  - `alaErpRingPortIfIndex`
  - `alaErpRingPortClearStats`
show erp

Displays the ERP configuration information for all rings, a specific ring, or for a specific ring port.

show erp [ring ring_id | port chassis/slot/port | linkagg agg_id]

Syntax Definitions

- **ring_id**: An existing ERP ring ID number. The valid range is 1 to 2147483647.
- **chassis**: The chassis identifier.
- **slot/port**: The slot number for the module and the physical port number on that module.
- **agg_id**: The link aggregate ID number.

Defaults

By default, configuration information is displayed for all ERP rings in the switch configuration.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Enter a ring ID to display the configuration for a specific ring.
- Enter a ring port number or a link aggregate ID to display the configuration for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.

Examples

```
-> show erp
Legends: * to Inactive Configuration
         WTR to Wait To Restore
         MEG to Maintenance Entity Group

Ring  Ring  Ring  Ring  Serv  WTR  Guard  MEG  Ring   Ring  Ring  Remote
ID   Port1 Port2 Status VLAN Timer Timer Level State Node Profile System ID (min) (csec)
-----+-------+-------+--------+-----+---+-----+-----+--------+-------+--------+------------+-------+-------+-----------+
  1   1/1/1 1/1/2  enabled   10  5  50  1   protection non-rpl  N/A       N/A
  2   1/1/3 1/1/4  enabled   100 5  50  1  protection non-rpl      SAP-SAP  N/A       N/A
  3   1/1/5 1/1/6  enabled   200 5  50  1  protection non-rpl      SAP-SDP 11:22:33:44:55:66
Total number of rings configured = 3
```
-> show erp ring 2
Legend: * to Inactive Configuration
Ring Id : 2,
Ring Type : Normal Ring,
Ring Port1 : 1/1/3,
Ring Port2 : 1/1/4,
Ring Status : enabled,
Service VLAN : 10,
Revertive Mode : enable,
WTR Timer (min) : 5,
Guard Timer (centi-sec) : 50,
Virtual Channel : enable,
MEG Level : 1,
Ring State : protection,
Active ERP version : Ver 2,
Ring Node Type : non-rpl,
Ring Profile : SAP-SAP,
Last State Change : Mon Jun 29 2020 22:21:49  (sysUpTime 2d:06h:41m)

output definitions
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring ID</td>
<td>The ERP ring ID number.</td>
</tr>
<tr>
<td>Ring Type</td>
<td>The ERP ring type.</td>
</tr>
<tr>
<td>Ring Port1</td>
<td>The chassis, slot and port number of the ring port1.</td>
</tr>
<tr>
<td>Ring Port2</td>
<td>The chassis, slot and port number of the ring port2.</td>
</tr>
<tr>
<td>Ring Status</td>
<td>The ring status (enabled or disabled).</td>
</tr>
<tr>
<td>Service VLAN</td>
<td>The Service VLAN ID.</td>
</tr>
<tr>
<td>Revertive Mode</td>
<td>Indicates if the revertive mode on the specified node is enabled or disabled.</td>
</tr>
<tr>
<td>WTR Timer</td>
<td>The wait-to-restore timer value in minutes for RPL node.</td>
</tr>
<tr>
<td>Guard Timer</td>
<td>The guard timer value in centi-secs for the ring node.</td>
</tr>
<tr>
<td>Virtual Channel</td>
<td>Indicates if ERP ring Virtual Channel is enabled or disabled.</td>
</tr>
<tr>
<td>MEG Level</td>
<td>The Service VLAN Management Entity Group (MEG) level.</td>
</tr>
<tr>
<td>Ring State</td>
<td>Indicates the state of the ring.</td>
</tr>
<tr>
<td>Active ERP version</td>
<td>Indicates the active ERP version.</td>
</tr>
<tr>
<td>Ring Node Type</td>
<td>Indicates the type of the ring node.</td>
</tr>
<tr>
<td>Ring Profile</td>
<td>The profile of the ring (N/A, SAP-SAP, SAP-SDP).</td>
</tr>
<tr>
<td>Last State Change</td>
<td>Indicates the time when the last state change occurred.</td>
</tr>
</tbody>
</table>

-> show erp port 1/1/2
Ring-Id : 1
  Ring Port Status : blocking,
  Ring Port Type : non-rpl,
  Ethoam Event : disabled,
  Remote-endpoint Id : none
  SPB SAP Neighbor : no
-> show erp linkagg 1
Ring-Id : 1
  Ring Port Status : blocking,
  Ring Port Type   : non-rpl,
  Ethoam Event    : disabled,
  Remote-endpoint Id : none
SPB SAP Neighbor : yes (or no)

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring ID</td>
<td>The ERP ring ID number.</td>
</tr>
<tr>
<td>Ring Port Status</td>
<td>The status of the ring port (blocking or forwarding).</td>
</tr>
<tr>
<td>Ring Port Type</td>
<td>The type of ring port.</td>
</tr>
<tr>
<td>Ethoam Event</td>
<td>Indicates whether or not the ring port will accept Ethernet OAM loss of</td>
</tr>
<tr>
<td></td>
<td>connectivity events (enabled or disabled).</td>
</tr>
<tr>
<td>Remote-endpoint Id</td>
<td>The remote Ethernet OAM MEP ID number from which this port accepts loss of</td>
</tr>
<tr>
<td></td>
<td>connectivity events. This field displays only when the ring port is</td>
</tr>
<tr>
<td></td>
<td>configured to receive such events.</td>
</tr>
<tr>
<td>SPB Remote-system Id</td>
<td>MAC address of the remote system of the BEB where the other end of the</td>
</tr>
<tr>
<td></td>
<td>ERP ring is connected as the access port.</td>
</tr>
<tr>
<td>SPB SAP Neighbor</td>
<td>Indicates if SPB SAP neighbor is configured or not.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 8.8R1; **Ring Profile, Remote System ID, SPB SAP Neighbor** fields added.

**Related Commands**

- `show erp statistics` Displays ERP ring statistics.

**MIB Objects**

alaErpRingId
alaErpRingStatus
alaErpRingServiceVid
alaErpRingMEGLevel
alaErpRingPort1
alaErpRingPort2
alaErpRingPortIfIndex
alaErpRingState
alaErpRingPortStatus
alaErpRingPortType
alaErpRingPortEthOAMEvent
alaErpRingPortRmepId
alaErpRingWaitToRestoreTimer
alaErpRingGuardTimer
alaErpRingLastStateChange
alaErpRingTimeToRevert
alaErpRingPortProfile
alaErpRingPort1ServiceVlanTagStatus
alaErpRingPort2ServiceVlanTagStatus
alaErpRingSpbRemoteId
alaErpRingPortIsSAPNeighbor
**show erp statistics**

Displays the ERP statistics for all rings, a specific ring, or a specific ring port.

```plaintext
show erp statistics [ring ring_id [port chassis/slot/port | linkagg agg_id]]
```

### Syntax Definitions

- **ring_id**: An existing ERP ring ID number. The valid range is 1 to 2147483647.
- **chassis**: The chassis identifier.
- **slot/port**: The slot number for the module and the physical port number on that module.
- **agg_id**: The link aggregate ID number.

### Defaults

By default, statistics are displayed for all ERP rings in the switch configuration.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860M</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a ring ID to display the statistics for a specific ring.
- Enter a ring ID and a ring port number or link aggregate ID to display the statistics for a specific port or link aggregate.
- The specified ring ID must exist in the switch configuration.
- The specified port must belong to the ring identified by the ring ID.

### Examples

```plaintext
-> show erp statistics
Legends: R-APS to Ring Automatic Protection Switching  
RPL to Ring Protection Link

Ring-Id : 1
Ring Port : 1/15
Signal Fail PDUs
  Sent : 3,
  Recv : 0,
  Drop : 0
No Request PDUs
```
show erp statistics

Sent : 37,
Recv : 37,
Drop : 0
No Request RPL Block PDUs
   Sent : 4322,
   Recv : 0,
   Drop : 0
Invalid R-APS PDUs
   Recv : 0

Ring Port : 1/1
Signal Fail PDUs
   Sent : 6,
   Recv : 0,
   Drop : 0
No Request PDUs
   Sent : 37,
   Recv : 38,
   Drop : 0
No Request RPL Block PDUs
   Sent : 4322,
   Recv : 0,
   Drop : 0
Invalid R-APS PDUs
   Recv : 0

Ring Id : 2
Ring Port : 6/7
Signal Fail PDUs
   Sent : 6,
   Recv : 0,
   Drop : 0
No Request PDUs
   Sent : 16,
   Recv : 14,
   Drop : 0
No Request RPL Block PDUs
   Sent : 4347,
   Recv : 0,
   Drop : 4341
Invalid R-APS PDUs
   Recv : 0

-> show erp statistics ring 3
Legends: R-APS  to Ring Automatic Protection Switching
         RPL    to Ring Protection Link

Ring Id : 3
Ring Port : 4/7
Signal Fail PDUs
   Sent : 6,
   Recv : 0,
   Drop : 0
No Request PDUs
   Sent : 16,
   Recv : 14,
   Drop : 0
No Request RPL Block PDUs
Sent : 4351,
Recv : 0,
Drop : 0
Invalid R-APS PDUs
Recv : 0

Ring Port : 6/1
Signal Fail PDUs
Sent : 6,
Recv : 0,
Drop : 0
No Request PDUs
Sent : 13,
Recv : 13,
Drop : 0
No Request RPL Block PDUs
Sent : 4358,
Recv : 0,
Drop : 0
Invalid R-APS PDUs
Recv : 0

-> show erp statistics ring 1 port 1/15
Legends: R-APS to Ring Automatic Protection Switching
RPL to Ring Protection Link

Ring-Id : 1
Ring Port : 1/15
Signal Fail PDUs
Sent : 3,
Recv : 0,
Drop : 0
No Request PDUs
Sent : 37,
Recv : 37,
Drop : 0
No Request RPL Block PDUs
Sent : 4338,
Recv : 0,
Drop : 0
Invalid R-APS PDUs
Recv: 0

output definitions

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ring ID</td>
<td>The ERP ring ID number.</td>
</tr>
<tr>
<td>Ring Port</td>
<td>The slot and port number of the ring port.</td>
</tr>
<tr>
<td>R-APS</td>
<td>The type of Ring Automatic Switching Protocol (R-APS) event message. NR = no request, RB = RPL is blocked, SF = signal failure. APS is the protocol ERP uses to monitor and control ring links.</td>
</tr>
<tr>
<td>Send</td>
<td>Total number of R-APS messages sent.</td>
</tr>
<tr>
<td>Recv</td>
<td>Total number of R-APS messages received.</td>
</tr>
<tr>
<td>Drop</td>
<td>Total number of R-APS messages dropped.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **show erp** Displays the ERP ring configuration for the switch.
- **clear erp statistics** Clears ERP ring statistics.

**MIB Objects**

- `alaERPClearStats`
- `alaERPRingClearStats`
- `alaErpRingPortClearStats`
- `alaErpRingId`
  - `alaErpRingPortIfIndex`
  - `alaErpStatsSignalFailPduTx`
  - `alaErpStatsSignalFailPduRx`
  - `alaErpStatsSignalFailPduDrop`
  - `alaErpStatsNoRequestPduTx`
  - `alaErpStatsNoRequestPduRx`
  - `alaErpStatsNoRequestPduDrop`
  - `alaErpStatsRPLBlockPDUtx`
  - `alaErpStatsRPLBlockPDUrx`
  - `alaErpStatsRPLBlockPDUdrop`
  - `alaErpStatsPDUerr`
15 Media Redundancy Protocol Commands

Media Redundancy Protocol (MRP) is an IEC standard that specifies a recovery protocol for use in high availability ring topology networks used in industrial automation networks. It is described in the IEC 62439-2. The protocol is designed to react to a single link or switch failure in the network and provide deterministic recovery time, which is important in ensuring real time data communication needs of industrial networks. During the failure of a connection, the media redundancy reconfigures the network so that the nodes can be accessed again through a substitute path.

MIB information for MRP commands is as follows:

Filename: IEC-62439-2-MIB.mib, ALCATEL-IND1-MRP-MIB.mib
Module: IEC62439, alcatelIND1MRPMIB

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>MRP Domain and Interconnection commands</th>
<th>mrp</th>
<th>mrp domain</th>
<th>mrp inter connect</th>
<th>show mrp</th>
<th>show mrp domain</th>
<th>show mrp port</th>
<th>show mrp interconnect</th>
<th>clear mrp</th>
<th>clear mrp port</th>
<th>clear mrp interconnect</th>
</tr>
</thead>
</table>


mrp

Configures a Domain or Interconnection with VLAN ID for the MRP ring.

mrp {domain domain_index | interconnect interconnect_id} vlan vlan_id

no mrp {domain domain_index | interconnect interconnect_id}

Syntax Definitions

domain_index
The domain identifier unique in the switch. The range is 1-3.
This key attribute defines the redundancy domain representing the MRP ring.

interconnect_id
Specifies the interconnection identifier unique in the switch. This is a
mandatory parameter to create a MRP interconnection. Allowed values are 1 to 65535.

vlan_id
The service VLAN ID number of the MRP ring. The valid range is 2 to 4094. Control traffic will flow with this VLAN tag in the ring.

Defaults
None.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- MRP is packaged into a Debian package, which can be installed on the switch. To configure MRP in AoS, it is required to install the MRP package using Package Manager commands. For more information on the Package Manager, see “Chassis Management and Monitoring Commands” chapter in the OmniSwitch AOS Release 8 CLI Reference Guide.

- MRP is supported in a standalone mode (virtual chassis of one) on OmniSwitch 6465. MRP is supported on virtual chassis of one or more on OmniSwitch 6865.

- Use the no form of this command to remove a ring from the switch configuration.

- A maximum of three MRP rings (domain) will be supported at a time in a node. Also, a node can have MRM/MRA (Media Redundancy Manager/Media Redundancy Auto-manager) role for only one ring among the allowed three rings.

- MRP domain configuration is mandatory to enable MRP interconnect on a switch.
• Specify a static VLAN ID for the MRP service VLAN; dynamic VLANs are not configurable as service VLANs.

• The service VLAN can belong to only one MRP ring at a time. The specified service VLAN ID must not participate in a Spanning Tree instance that is associated with non-MRP VLANs. Ideally, change the Spanning Tree configuration for the VLAN ID prior to using this command.

• VLAN used to create MRP must not be deleted till the MRP configuration is removed.

• STP will be disabled on MRP ring ports.

• MRP or ERP, any one of the redundancy protocol work at a time.

• MRP is not supported on mobile ports, mirroring ports, VFL port, UNI port, LPS port, UNP port, DHL port, or Openflow ports.

Examples

-> mrp domain 1 vlan 10

-> mrp interconnect 1 vlan 10

-> no mrp domain 1

Release History

Release 8.7R2; command introduced.
Release 8.9R1; mrp interconnect support added.

Related Commands

mrp domain
Configures the MRP ring parameters like domain index, ring ports, admin-role, priority, react on link change, and recovery. Use this command to administratively enable or disable an MRP ring.

mrp inter connect
Configures the MRP interconnection parameters like interconnection index, interconnection ports, admin-role, mode, and recovery time.

show mrp
Displays the MRP configuration information.

MIB Objects

mrpDomainTable
    mrpDomainIndex
    mrpDomainVlanId
    mrpDomainState
**mrp domain**

Configures the MRP ring parameters, such as domain index, ring ports, admin-role, priority, react on link change, and recovery. Use this command to administratively enable or disable an MRP ring.

```
mrp domain domain_index [name domain_name] [uuid uuid] port1 {linkagg agg_id | chassis/slot/port | slot/port} port2 {linkagg agg_id | chassis/slot/port | slot/port} [admin-role {client | manager | auto-manager}] [manager {priority priority | linkchange-react {enable | disable} | test-default [{interval interval | count repeat_count}] | [rt-delay-reset] [recovery-time {500ms | 200ms | 30ms | 10ms}]]
mrp domain domain_index admin-state {enable | disable}
```

**Syntax Definitions**

- **domain_index**
  Specifies the domain identifier unique in the switch. The range is 1–3.

- **domain_name**
  Specifies a logical name for the MRP domain to ease the management of MRP domains. The maximum length is up to 18 characters.

- **uuid**
  Specifies the unique 16 hexadecimal domain ID.

- **port1**
  The interface ID of the first ring port, which is either a bridge port, or an aggregated link within a bridge on which the ring is configured. There can be only two ring ports per ring in a bridge.

- **agg_id**
  A link aggregate ID number.

- **chassis**
  The chassis identifier.

- **slot/port**
  The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

- **port2**
  The interface ID of the second ring port, which is either a bridge port, or an aggregated link within a bridge on which the ring is configured. There can be only two ring ports per ring in a bridge.

- **client | manager | auto-manager**
  Specifies the role of the node redundancy domain.
  - By choosing the admin-role Manager, the device becomes the redundancy manager, MRM (Media Redundancy Manager).
  - By choosing the admin-role Client, the device becomes the redundancy client, MRC Media Redundancy Client).
  - By choosing the admin-role Auto-manager, the device becomes the redundancy auto-manager, MRA (Media Redundancy Auto-manager).

- **priority**
  The priority of the MRP entity. Lesser the value, higher the priority. The valid range is 0–65535.

- **linkchange-react enable**
  Specifies the MRM/MRA to react immediately on link-down MRP link change frames from MRC.

- **linkchange-react disable**
  Specifies the MRM/MRA to not react on link-down MRP link change frames from MRC.

- **interval**
  Specifies the test default timer for sending the MRP test frames to MRM/MRA in milliseconds. The range is 20–125.

  Test default interval range for 200ms recovery time is 20–50, and for 500ms recovery time is 50–125.
**repeat_count**
- Specifies the test default repeat count for MRM/MRA. The valid range is 1–15.

**rt-delay-reset**
- Resets the values of maximum round-trip-delay and minimum and round-trip-delay to zero at the same time.

**recovery-time**
- Specifies the maximum recovery time of a ring in milliseconds. Only 200ms and 500ms recovery time is supported.

**enable**
- Enables the administrative state of the MRP ring.

**disable**
- Disables the administrative state of the MRP ring.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>domain_name</strong></td>
<td>DOMAIN-X, where X is domain ID.</td>
</tr>
<tr>
<td><strong>uuid</strong></td>
<td>0xFFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFF (for domain ID 1)</td>
</tr>
<tr>
<td></td>
<td>0xFFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFE (for domain ID 2)</td>
</tr>
<tr>
<td></td>
<td>0xFFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFD (for domain ID 3)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>**client</th>
<th>manager</th>
<th>auto-manager**</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>priority</strong></td>
<td>0x8000 - for MRM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0xA000 - for MRA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>linkchange-react</strong></th>
<th>enable</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th><strong>interval</strong></th>
<th>50ms for 200ms recovery time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>80ms for 500ms recovery time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>repeat_count</strong></th>
<th>3 for 200ms recovery time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5 for 500ms recovery time</td>
</tr>
</tbody>
</table>

| **10ms | 30ms | 200ms | 500ms** | 200ms |

<table>
<thead>
<tr>
<th>**enable</th>
<th>disable**</th>
<th>default</th>
</tr>
</thead>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
Usage Guidelines

- All devices in a ring which are configured with MRP must be part of the same redundancy domain. The domain is identified by domain identifier or domain name.
- Each specified ring port can only be part of a single ring.
- The maximum number of nodes in a ring is 50.
- A maximum of three MRP rings (domain) will be supported at a time in a node. Also, a node can have MRM/MRA role for only one ring among the allowed three rings.
- To configure Manager parameters (like priority, linkchange-react, test-default interval and so on), admin-role Manager or Auto-Manager must be configured first.
- Test default interval, repeat count, and recovery time must be same for all the switches in the domain.
- MRP ring supports multicast L2 and L3 flows; and the flows are converged within the configured recovery time and static multicast convergence time of a ring with static multicast querier and static multicast neighbor configuration.
- In MRP closed domain, blocking ports on MRM will go in STP blocking for all the VLANs configured on this port. VLANs which are not part of ring will also be affected due to this.
- MRAs select one MRM among each other by using a voting protocol. The remaining MRAs transition to the role MRC.
- If any of the node in the ring is configured as MRM, then all the nodes in ring that are configured with auto-manager moves to client role, MRC.
- The MRP priority value is used in the voting process to decide which of the nodes will finally become the MRM, while the other nodes take over the MRC role.
- STP will be disabled on the configured MRP ring ports once MRP ring is administratively enabled.

Examples

-> mrp domain 1 uuid 0xffffffff-ffff-ffff-ffff-ffffffffffe
-> mrp domain 1 port1 linkagg 1 port2 1/1/1 admin-role client recovery-time 200ms
-> mrp domain 1 name domain-2 port1 linkagg 1 port2 1/1/1 admin-role manager rt-delay-reset recovery-time 200ms
-> mrp domain 1 manager priority 10 linkchange-react enable test-default interval 50
-> mrp domain 1 admin-state enable
-> no mrp domain 1

Release History

Release 8.7R2; command introduced.
**Related Commands**

- **mrp**
  Configures a domain with VLAN ID for the MRP ring.

- **show mrp domain**
  Displays the MRP domain configuration information for a specific ID, domain name, or UUID.

- **show mrp**
  Displays the MRP configuration information.

**MIB Objects**

- `mrpDomainTable, alaMrpDomainTable`
- `mrpDomainIndex`
- `mrpDomainName`
- `mrpDomainID`
- `mrpDomainRingPort1`
- `mrpDomainRingPort2`
- `mrpDomainAdminRole`
- `mrpDomainManagerPriority`
- `mrpDomainMRMReactOnLinkChange`
- `alaMRPDomainMRMTestDefaultInterval`
- `alaMRPDomainMRMTestNRMax`
- `mrpDomainResetRoundTripDelays`
- `alaMrpDomainRecoveryTime`
**mrp interconnect**

Configures the MRP interconnection parameters like interconnection index, interconnection ports, admin-role, mode, and recovery time.

Use this command to administratively enable or disable an MRP interconnection ring.

```
mrp interconnect interconnect_id [name name] port {linkagg agg_id | chassis/slot/port | slot/port} [admin-role {client | manager}] [manager {test-default [{interval interval | count repeat_count}] | [mode {link-check | ring-check}] [recovery-time {500ms | 200ms | 30ms | 10ms}]]
mrp interconnect interconnect_id admin-state {enable | disable}
```

### Syntax Definitions

- **interconnect_id**: Specifies the interconnection identifier unique in the switch. This is a mandatory parameter to create a MRP interconnection. Allowed values are 1 to 65535.
- **name**: Specifies an unique name for the redundant interconnection domain of MRP rings. The maximum length is up to 240 characters.
- **port**: The interface index of the interconnection port, which is either a bridge port, or an aggregated link within a bridge.
- **agg_id**: A link aggregate ID number.
- **chassis**: The chassis identifier.
- **slot/port**: The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
- **client | manager**: Specifies the role of the node.
  - By choosing the admin-role Manager, the device becomes the redundancy manager, MIM (Media Redundancy Interconnection Manager).
  - By choosing the admin-role Client, the device becomes the redundancy client, MIC (Media Redundancy Interconnection Client).
- **interval**: Specifies the test default timer for sending the MRP interconnect test frames to MIM in milliseconds. The range is 20–125.
  - Test default interval range for 200ms recovery time is 20–50, and for 500ms recovery time is 50–125.
- **repeat_count**: Specifies the test default repeat count for MIM. The valid range is 1–15.
- **link-check | ring-check**: Specifies the mode.
  - The MIM can observe the interconnection topology by either reacting directly on interconnection port link change notification messages (LC-mode) or by sending test frames on the interconnection port over the connected rings and receiving them over its ring ports, and vice versa in the other direction (RC mode).
- **recovery-time**: Specifies the maximum recovery time of a ring in milliseconds.
  - Only 200ms and 500ms recovery time is supported.
- **enable**: Enables the administrative state of the MRP ring.
- **disable**: Disables the administrative state of the MRP ring.
**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>INTERCONNECTION-&lt;id&gt;</td>
</tr>
<tr>
<td>client</td>
<td>manager</td>
</tr>
<tr>
<td>interval</td>
<td>50ms for 200ms recovery time 80ms for 500ms recovery time</td>
</tr>
<tr>
<td>repeat_count</td>
<td>3 for 200ms recovery time 5 for 500ms recovery time</td>
</tr>
<tr>
<td>link-check</td>
<td>ring-check</td>
</tr>
<tr>
<td>10ms</td>
<td>30ms</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Each specified ring port can only be part of a single ring.
- MRP domain configuration is mandatory to enable MRP interconnect on a switch.
- VLAN used to configure MRP interconnection should not be deleted until MRP Interconnect configuration is removed. MRP interconnect will be disabled if VLAN or VPA for service VLAN is removed.
- Test default interval, repeat count, and recovery time must be same for all the switches in the domain.
- MRP interconnect ring will consist of four nodes. Among these nodes, one node will be MIM, and the remaining will be MIC.
- On both OmniSwitch 6465 and OmniSwitch 6865, only one Domain and two Interconnects (or one Interconnect) is supported.
- On OmniSwitch 6465,
  - with MRM as Base Domain, RC mode is not allowed. In LC mode, only one Interconnect is supported (MIM/MIC).
  - with MRC as Base Domain, both LC and RC modes are allowed but only one Interconnect is supported (MIM/MIC).
- On OmniSwitch 6865,
  - with MRM as Base Domain, RC mode is not allowed with MIM configuration. MIM + MIM
configuration is not allowed in both LC and RC mode.
- with MRC as Base Domain, both LC and RC modes are allowed. MIM + MIM configuration is not allowed in both LC and RC mode.

- Use **no** command to delete an existing MRP interconnection.

### Examples

```
-> mrp interconnect 1 port1 linkagg 1 admin-role manager manager test-default
   interval 50 mode link-check recovery-time 200ms

-> mrp interconnect 1 vlan 10 admin-state enable

-> no mrp interconnect 1
```

### Release History

Release 8.9R1; command introduced.

### Related Commands

- **mrp**
  - Configures a domain with VLAN ID for the MRP ring.

- **show mrp interconnect**
  - Displays the MRP domain configuration information for a specific interconnection ID or name.

- **show mrp**
  - Displays the MRP configuration information.

### MIB Objects

- `mrpInterconnectionTable`
- `alaMrpInterconnectionTable`
- `mrpInterconnectionID`
- `mrpInterconnectionName`
- `mrpInterconnectionPort`
- `mrpInterconnectionPortState`
- `mrpInterconnectionVlanId`
- `mrpInterconnectionMode`
- `mrpInterconnectionAdminRole`
- `mrpInterconnectionOperRole`
- `mrpInterconnectionState`
- `mrpInterconnectionError`
- `mrpInterconnectionOpenCount`
- `mrpInterconnectionLastOpenChange`
- `mrpInterconnectionPeerMAC`
- `mrpInterconnectionOwnMRMMAC`
- `mrpInterconnectionPeerMRMMAC`
- `mrpInterconnectionPeerRingDomainUUID`
- `alaMRPInterconnectionAdminState`
- `alaMRPInterconnectionRecoveryTime`
- `alaMRPInterconnectionMIMTopChangeInterval`
- `alaMRPInterconnectionMIMTopChangeNRMax`
- `alaMRPInterconnectionMIMTestDefaultInterval`
- `alaMRPInterconnectionMIMTestNRMax`
- `alaMRPInterconnectionMIMStatusPollInterval`
- `alaMRPInterconnectionMIMStatusPollNRMax`
- `alaMRPInterconnectionMICLinkUpInterval`
- `alaMRPInterconnectionMICLinkDownInterval`
- `alaMRPInterconnectionMICLinkUpNRMax`
alaMRPInterconnectionMICLinkDownNRMax
alaMRPInterconnectionPortMAC
**show mrp**

Displays the MRP configuration information.

**show mrp [domain [\{id | name name | uuid uuid\}]]**

### Syntax Definitions

- **id**
  The domain identifier unique in the switch. When specified, displays the MRP domain configuration for a MRP domain.

- **name**
  The domain name. When specified, displays the MRP domain configuration for a specific MRP domain name.

- **uuid**
  The 16 hexadecimal domain ID. When specified, displays the MRP domain configuration for a specific UUID.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support for show mrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/ X48C8/C32E/T24C2/ X24C2</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

**MRM/MRC/MRA:**

```
-> show mrp
Domain Port1 Port2 Status State Config Operational VLAN Recovery time (ms)
---+-------+---------------+--------+------------+-----------+----+-----------
 1  0/10*  1/1/23  Enabled  Close    Manager    Manager    100    200
 2  0/20*   0/21    Enabled  Undefined  Client     Client     200    200
 3    1/1/24  0/35*   Enabled  Undefined  Client     Client     300    200

* - MRP selected primary port
On MRP Manager, Secondary port is Blocking in Closed state and Forwarding in Open state.
```

### Domain Information

<table>
<thead>
<tr>
<th>Domain</th>
<th>Domain UUID</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0xffffffff-ffff-ffff-ffff-ffffffffffff</td>
<td>DOMAIN-1</td>
</tr>
</tbody>
</table>
With Interconnect:

-> show mrp

<table>
<thead>
<tr>
<th>Domain</th>
<th>Config Role</th>
<th>Operational Role</th>
<th>VLAN</th>
<th>Recovery time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain-2</td>
<td>Client</td>
<td>Client</td>
<td>30</td>
<td>200</td>
</tr>
</tbody>
</table>

*- MRP selected primary port

On MRP Manager, Secondary port is blocking in Closed state and Forwarding in Open state.

<table>
<thead>
<tr>
<th>Domain Id</th>
<th>Domain UUID</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>0xffffffff-ffff-ffff-ffff-fffffffffffe</td>
<td>DOMAIN-2</td>
</tr>
</tbody>
</table>

Total Number of Rings : 1

Interconnection ID: 1 | Name: mrp_in1

<table>
<thead>
<tr>
<th>Port</th>
<th>Port state</th>
<th>Mode</th>
<th>Status</th>
<th>State</th>
<th>Role</th>
<th>VLAN</th>
<th>Recovery time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>Forwarding</td>
<td>LC</td>
<td>Disable</td>
<td>Open</td>
<td>Manager</td>
<td>50</td>
<td>500</td>
</tr>
</tbody>
</table>

Last State Change : Tuesday, August 11, 1970, 09h:41m:10s, 5

Interconnection Open Count : 10

Interconnection peer MAC : 00:d0:95:11:11:16

Interconnection own MRM MAC : 00:d0:95:11:11:12

Interconnection Elected MIM MAC : 2c:fa:a2:9a:92:29

Interconnection peer domain UUID : 0x00000000-0000-0000-0000-000000000002

Total Number of Rings : 1

Total Number of Interconnections: 1

output definitions

**Domain Id**
A unique ID that represents the MRP ring.

**Port1**
Port ID that serves as the first ring port:

**Port2**
Port ID that serves as the second ring port:

**Status**
Administrative status of the MRP ring.

**State**
The MRP ring state: open, close, undefined

**Config Role**
The role of the node redundancy domain.

**Operational Role**
The operational role of the node.

**VLAN**
The VLAN for sending MRP frames.

**Recovery time (ms)**
The maximum recovery time of a ring in milliseconds.

**Domain UUID**
The UUID of the MRP redundancy domain.

**Domain Name**
The the domain name of the configured MRP ring.

**Interconnection ID**
A unique interconnection ID that represents the MRP ring.

**Name**
An unique name for the redundant interconnection of MRP rings.

**Last State Change**
Timeticks since last change of mrpInterconnectionState to interconnOpen.
### Release History

Release 8.7R2; command introduced.

### Related Commands

- **show mrp domain**
  
  Displays the MRP domain configuration information for a specific ID, domain name, or UUID.

- **show mrp interconnect**
  
  Displays the MRP interconnection configuration information for a specific interconnection ID or name.

- **show mrp port**
  
  Displays the packet counters for an MRP domain for a specific port or a linkagg.

### MIB Objects

- mrpDomainIndex
- mrpDomainID
- mrpDomainState
- mrpDomainAdminRole
- mrpDomainOperRole
- mrpDomainVlanId
- alaMRPDomainRecoveryTime
- mrpDomainRingPort1
- mrpDomainRingPort1State
- mrpDomainRingPort2
- mrpDomainRingPort2State
- mrpDomainName
- mrpDomainError
- mrpDomainManagerPriority
- mrpDomainRingOpenCount
- mrpDomainLastRingOpenChange
- mrpDomainRoundTripDelayMax
- mrpDomainRoundTripDelayMin
- alaMRPDomainElectMRMMAC
- alaMRPDomainPort1MAC
- alaMRPDomainPort2MAC
- alaMRPDomainHostMRMMAC
- alaMRPDomainElectMRMPriority

---

**output definitions (continued)**

<table>
<thead>
<tr>
<th><strong>Interconnection Open Count</strong></th>
<th>Counter for MRP Interconnection state changes to interconnOpen.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interconnection peer MAC</strong></td>
<td>Device MAC address of the devices interconnection peer, connected to the devices interlink port.</td>
</tr>
<tr>
<td><strong>Interconnection own MRM MAC</strong></td>
<td>The device MAC address of the devices ring manager (MRM).</td>
</tr>
<tr>
<td><strong>Interconnection Elected MIM MAC</strong></td>
<td>The switch MAC address of the elected MIM.</td>
</tr>
<tr>
<td><strong>Interconnection peer domain UUID</strong></td>
<td>The domain UUID of the ring the interconnection peer's, connected to the devices interlink port, ring.</td>
</tr>
<tr>
<td><strong>Total Number of Rings</strong></td>
<td>Total number of MRP rings.</td>
</tr>
<tr>
<td><strong>Total Number of Interconnections</strong></td>
<td>Total number of interconnection domain rings.</td>
</tr>
</tbody>
</table>
show mrp

- mrpInterconnectionID
- mrpInterconnectionName
- mrpInterconnectionPort
- mrpInterconnectionPortState
- mrpInterconnectionVlanId
- mrpInterconnectionMode
- mrpInterconnectionAdminRole
- mrpInterconnectionOperRole
- mrpInterconnectionState
- mrpInterconnectionError
- mrpInterconnectionOpenCount
- mrpInterconnectionLastOpenChange
- mrpInterconnectionPeerMAC
- mrpInterconnectionOwnMRMMAC
- mrpInterconnectionPeerMRMMAC
- mrpInterconnectionPeerRingDomainUUID
- alaMRPInterconnectionAdminState
- alaMRPInterconnectionRecoveryTime
- alaMRPInterconnectionMIMtopChangeInterval
- alaMRPInterconnectionMIMtopChangeNRMax
- alaMRPInterconnectionMIMtestDefaultInterval
- alaMRPInterconnectionMIMtestNRMax
- alaMRPInterconnectionMIMstatusPollInterval
- alaMRPInterconnectionMIMstatusPollNRMax
- alaMRPInterconnectionMIClinkUpInterval
- alaMRPInterconnectionMIClinkDownInterval
- alaMRPInterconnectionMIClinkUpNRMax
- alaMRPInterconnectionMIClinkDownNRMax
- alaMRPInterconnectionPortMAC
show mrp domain

Displays the MRP domain configuration information for a specific ID, domain name, or UUID.

show mrp domain [{domain_index | name name} | uuid uuid] [counters] [detail] [elected-manager] [ring-port] [rt-delay]

Syntax Definitions

domain_index
The domain identifier unique in the switch. When specified, displays the MRP domain configuration for a MRP domain.

name
The domain name. When specified, displays the MRP domain configuration for a MRP domain name.

uuid
The 16 hexadecimal domain ID. When specified, displays the MRP domain configuration for a specific UUID.

counters
Display the counters for a specific domain ID, domain name, or UUID.

detail
Display the MRP domain configuration in detail for a specific domain.

elected-manager
Display the elected-manager source MAC and priority.

ring-port
Display the ring ports belonging to a specific domain.

rt-delay
Display the round-trip-delay for a specific domain. This is applicable only for MRM/MRA.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900 X32E/T24C2/ X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show mrp domain

<table>
<thead>
<tr>
<th>Domain</th>
<th>Config</th>
<th>Operational</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Port1</td>
<td>Port2</td>
<td>Status</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>1</td>
<td>0/10*</td>
<td>1/1/23</td>
<td>Enabled</td>
</tr>
<tr>
<td>2</td>
<td>0/20*</td>
<td>0/21</td>
<td>Enabled</td>
</tr>
<tr>
<td>3</td>
<td>1/1/24</td>
<td>0/35*</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
*- MRP selected primary port
On MRP Manager, Secondary port is Blocking in Closed state and Forwarding in
Open state.

Domain
Id   Domain UUID                      Domain Name
-----------------------------------------------
1  0xffffffff-ffff-ffff-ffff-ffffffffffffff  DOMAIN-1
2  0xffffffff-ffff-ffff-ffff-ffffffffffffffe  DOMAIN-2
3  0xffffffff-ffff-ffff-ffff-fffffffffffffffd  DOMAIN-3

Total Number of Rings : 3

MRM:

-> show mrp domain
domain Id = 1
domain
Id   Status   State    Role      Role      VLAN  Time(ms)  Support     STM State
------+--------+--------+----------+-----+-----+---------+---------+-----------
1      Enabled   Close    Manager  Manager    100  200        TRUE       CHK_RC

Port Details:
Port   Port Type   Port Status    Port MAC
------+-----------+-------------+-----------------
0/10  Primary     Forwarding    2c:fa:a2:0a:39:72
1/1/23 Secondary   Blocked       2c:fa:a2:0a:39:84

Domain UUID            :   0xffffffff-ffff-ffff-ffff-ffffffffffffff
Domain Name            :   DOMAIN-1
Last State Change      :   Monday, September 28, 2020, 10h:46m:18s, 82
System Up Time         :   Monday, September 28, 2020, 10h:44m:48s
Elected MRM Source MAC :   2c:fa:a2:0a:39:67
Elected MRM Priority   :   32768 (0x8000)
Host Source MAC        :   2c:fa:a2:0a:39:67
Total number of rings  :   3
Error                  :   -
React on link change   :   Enable
Priority               :   32768 (0x8000)
Test Default Interval  :   50ms
Test NRMAX Count       :   3

RT-Delay            Min           Max          Ring Open
Total rx   Total tx   RT-Delay(µs) RT-Delay(µs)     Count
----------+----------+------------+------------+------------
0          0           33         1059        3

-> show mrp domain counters
Port1: 1/1/10
Type                Tx                  Rx                   Drop
------------------+----------------------+----------------------+-----------------
Test Frames                6835                 6404                  0
Topology Change            9                    0                    0
Link Up                    0                    3                    0
Link Down                  0                    0                    0
Error                      0

Port2: 1/1/4
Type                Tx                  Rx                   Drop
------------------+----------------------+----------------------+-----------------
Test Frames            6835       6404       0
Topology Change        9          0         0
Link Up                0          1         0
Link Down              0          0         0
Error                  0

-> show mrp domain elected-manager
Domain Id: 1
Elected MRM Source MAC : 2c:fa:a2:0a:39:67
Elected MRM Priority  : 32768 (0x8000)
Host Source MAC       : 2c:fa:a2:0a:39:67
Host Priority         : 32768 (0x8000)

-> show mrp domain ring-port
ID  Status   Port  Port Type  Port Status     MAC
---+-------+------+---------+-----------+-----------------
1  Enabled 0/10  Primary    Forwarding 2c:fa:a2:0a:39:72
1  Enabled 1/1/23 Secondary Blocked 2c:fa:a2:0a:39:84
2  Enabled 0/20  Primary    Forwarding 2c:fa:a2:0a:39:7a
2  Enabled 0/21  Secondary    Forwarding 2c:fa:a2:0a:39:7b

The following will be displayed only for MRM/MRA node.

-> show mrp domain rt-delay
Domain  Domain                             RT-delay(µs)     Ring Open
Id      status   Total rx   Total tx     Min        Max      Count
------+--------+----------+----------+----------+----------+-----------
1      Enabled     0          0         28        10009      3

MRC:

-> show mrp domain 2 detail
Domain Id = 2
Domain                   Config   Operational       Recovery  Non-Block
Id     Status    State    Role      Role      VLAN  Time(ms)  Support     STM State
------+--------+--------+--------+----------+------+---------+---------+-----------
2      Enabled  Undefined  Client   Client     200     200     False      PT_IDLE

Port Details:
Port   Port Type Port Status Port mac
------+---------+-----------+-----------------
1/1/10 Primary    Forwarding 2c:fa:a2:38:eb:b3
1/1/4 Secondary    Forwarding 2c:fa:a2:38:eb:ad

Domain UUID            : 0xffffffff-ffff-ffff-ffff-fffffffffffffffe
Domain Name            : DOMAIN-2
System Up Time         : Friday, March 13, 1970, 23h:06m
Elected MRM Source MAC : 00:00:00:00:00:00:00
Host Source MAC        : 2c:fa:a2:38:eb:a3
Total number of rings  : 1
Error                  : -

-> show mrp domain elected-manager
Domain Id: 1
Elected MRM Source MAC : 2c:fa:a2:9a:92:4f
Elected MRM Priority  : 32768 (0x8000)
Host Source MAC       : 2c:fa:a2:0a:39:67
**MRA:**

```
-> show mrp domain 1 detail
```

<table>
<thead>
<tr>
<th>Domain Id</th>
<th>Status</th>
<th>State</th>
<th>Config Role</th>
<th>Operational Role</th>
<th>VLAN</th>
<th>Recovery time (ms)</th>
<th>Non-Block Support</th>
<th>STM State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>Close</td>
<td>Auto-Manager</td>
<td>Manager</td>
<td>3015</td>
<td>200</td>
<td>TRUE</td>
<td>CHK_RC</td>
</tr>
</tbody>
</table>

**Port Details:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Port Type</th>
<th>Port Status</th>
<th>Port MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/10</td>
<td>Init</td>
<td>Blocked</td>
<td>2c:fa:a2:38:eb:b3</td>
</tr>
<tr>
<td>1/1/4</td>
<td>Init</td>
<td>Blocked</td>
<td>2c:fa:a2:38:eb:ad</td>
</tr>
</tbody>
</table>

- **Domain UUID:** 0xffffffff-ffff-ffff-ffff-fffffffffffffffe
- **Domain Name:** DOMAIN-2
- **Last State Change:** 0, Thursday, January 01, 1970, 00h:00m
- **System Up Time:** Friday, March 13, 1970, 23h:06m
- **Elected MRM Source MAC:** 2c:fa:a2:38:eb:a3
- **Elected MRM Priority:** 0x8000
- **Host Source MAC:** 2c:fa:a2:38:eb:a3
- **Total number of rings:** 1
- **Error:** -
- **React on link change:** Disable
- **Priority:** 0xA000
- **Test Default Interval:** 50ms
- **Test NRMAX Count:** 3

<table>
<thead>
<tr>
<th>RT-Delay</th>
<th>Min</th>
<th>Max</th>
<th>Ring Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total rx</td>
<td>0</td>
<td>0</td>
<td>33</td>
</tr>
</tbody>
</table>

**output definitions**

- **Domain Id**: A unique ID that represents the MRP ring.
- **Port1**: Port ID that serves as the first ring port.
- **Port2**: Port ID that serves as the second ring port.
- **Status**: Administrative status of the MRP ring.
- **State**: The MRP ring state: open, close, undefined
- **Config Role**: The role of the node redundancy domain.
- **Operational Role**: The operational role of the node.
- **VLAN**: The VLAN for sending MRP frames.
- **Recovery time (ms)**: The maximum recovery time of a ring in milliseconds.
- **Non-block support**: Support for blocking port for MRP control frames. MRC non-block support is **False**, and MRM non-block support is **True**.
- **STM State**: The protocol machine state.
- **Port**: The port ID.
- **Port Type**: The port type: primary or secondary.
- **Port Status**: The port state: blocking, forwarding, disabled.
### show mrp domain

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port mac</td>
<td>The port MAC address. In case of linkagg, it will be link aggregate primary port MAC address.</td>
</tr>
<tr>
<td>Domain UUID</td>
<td>UUID of the MRP redundancy domain.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Specifies the domain name of the configured MRP ring.</td>
</tr>
<tr>
<td>Last State Change</td>
<td>Timeticks since last change of ring-state close to ring open, and the time when the ring state is open.</td>
</tr>
<tr>
<td>System Up Time</td>
<td>The time of MRP configuration since the last system reboot.</td>
</tr>
<tr>
<td>Elected MRM Source MAC</td>
<td>The switch MAC address of the elected MRM.</td>
</tr>
<tr>
<td>Elected MRM Priority</td>
<td>The priority of the elected MRM.</td>
</tr>
<tr>
<td>Host Source MAC</td>
<td>The MAC address of the switch.</td>
</tr>
<tr>
<td>Total number of rings</td>
<td>Total number of rings in the switch.</td>
</tr>
<tr>
<td>Error</td>
<td>Displays the reason when the switch cannot reach to the desired administrative state.</td>
</tr>
<tr>
<td>React on link change</td>
<td>Enable: Indicates that the MRM reacts immediately on link up/down MRP link change frames. Disable: Indicates that the MRM will not react immediately on link up/down MRP link changes frames</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the MRM/MRA.</td>
</tr>
<tr>
<td>Test Default Interval</td>
<td>The default test interval.</td>
</tr>
<tr>
<td>Test NRMAX Count</td>
<td>The default test monitoring count.</td>
</tr>
<tr>
<td>Total rx</td>
<td>The total MRP control packets received.</td>
</tr>
<tr>
<td>Total tx</td>
<td>The total MRP control packets transmitted.</td>
</tr>
<tr>
<td>Min RT-Delay (µs)</td>
<td>The minimum round-trip-delay (in microseconds) that was measured since ring was administratively enabled.</td>
</tr>
<tr>
<td>Max RT-Delay (µs)</td>
<td>The maximum round-trip-delay (in microseconds) that was measured since ring was administratively enabled.</td>
</tr>
<tr>
<td>Ring Open Count</td>
<td>Number of times the ring moved to ring open state.</td>
</tr>
<tr>
<td>Type</td>
<td>MRP control frame type.</td>
</tr>
<tr>
<td>Tx</td>
<td>The number of MRP control frames transmitted.</td>
</tr>
<tr>
<td>Rx</td>
<td>The number of MRP control frames received.</td>
</tr>
<tr>
<td>Drop</td>
<td>The number of MRP control frames dropped.</td>
</tr>
<tr>
<td>Host Priority</td>
<td>The priority of the MRM/MRA.</td>
</tr>
<tr>
<td>Domain Id</td>
<td>A unique ID that represents the MRP ring.</td>
</tr>
<tr>
<td>Domain status</td>
<td>Operational state of the MRP ring.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.7R2; command introduced.
Media Redundancy Protocol Commands

show mrp domain

Related Commands

mrp domain
Configures the MRP ring parameters like domain index, ring ports, admin-role, priority, react on link change, and recovery.

show mrp
Displays the MRP configuration information.

MIB Objects

- mrpDomainIndex
- mrpDomainID
- mrpDomainName
- mrpDomainAdminRole
- mrpDomainOperRole
- mrpDomainRingPort1
- mrpDomainRingPort1State
- mrpDomainRingPort2
- mrpDomainRingPort2State
- mrpDomainState
- mrpDomainError
- mrpDomainVlanId
- mrpDomainManagerPriority
- mrpDomainRingOpenCount
- mrpDomainLastRingOpenChange
- mrpDomainRoundTripDelayMax
- mrpDomainRoundTripDelayMin
- alaMRPDomainElectMRMMAC
- alaMRPDomainPort1MAC
- alaMRPDomainPort2MAC
- alaMRPDomainHostMRMMAC
- alaMRPDomainElectMRMPriority
- alaMRPDomainRecoveryTime
- mrpDomainRoundTripDelayMax
- mrpDomainRoundTripDelayMin
- alaMRPRingPortIfIndex
- alaMRPDomainMRMRxTopChangeCounter
- alaMRPDomainMRMTxTopChangeCounter
- alaMRPDomainMRMRxDropTopChangeCounter
- alaMRPDomainMRMTxDropDefaultCounter
- alaMRPDomainMRMDropDefaultCounter
- alaMRPDomainMRMRxLinkUpCounter
- alaMRPDomainMRMCRxLinkUpCounter
- alaMRPDomainMRMCRxLinkDownCounter
- alaMRPDomainMRMCRxLinkDownCounter
- alaMRPDomainMRMACetherMAC
- alaMRPDomainMRMACetherMAC
- alaMRPDomainMRMACetherMAC
- alaMRPDomainMRMACetherMAC
- mrpDomainAdminRole
Media Redundancy Protocol Commands

show mrp domain

- mrpDomainOperRole
- mrpDomainVlanId
- alaMRPDomanRecoveryTime
**show mrp port**

Displays the packet counters for an MRP domain for a specific port or a linkagg.

`show mrp port {linkagg agg_id | chassis/slot/port} counters`

### Syntax Definitions

- **agg_id**: A link aggregate ID number.
- **chassis**: The chassis identifier.
- **slot/port**: The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
- **counters**: Display the counters for a port.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```bash
-> show mrp port 1/1/23 counters
Port2: 1/1/23
Type                Tx                   Rx                  Drop
------------------+----------------------+----------------------+-----------------
Test Frames               15628                15197                 0
Topology Change            9                    0                    0
Link Up                    0                    1                    0
Link Down                  0                    0                    0
Error                      0
```

#### output definitions

- **Type**: MRP control frame type.
- **Tx**: The number of MRP control frames transmitted.
output definitions (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx</td>
<td>The number of MRP control frames received.</td>
</tr>
<tr>
<td>Drop</td>
<td>The number of MRP control frames dropped.</td>
</tr>
</tbody>
</table>

Release History

Release 8.7R2; command introduced.

Related Commands

**show mrp**

Displays the MRP configuration information.

MIB Objects

alaMRPRingPortIfIndex
alaMRPDomainMRMRxTopChangeCounter
alaMRPDomainMRMTxTopChangeCounter
alaMRPDomainMRMDropTopChangeCounter
alaMRPDomainMRMRxTestDefaultCounter
alaMRPDomainMRMTxTestDefaultCounter
alaMRPDomainMRMDropTestDefaultCounter
alaMRPDomainMRCRxLinkUpCounter
alaMRPDomainMRCTxLinkUpCounter
alaMRPDomainMRCDropLinkUpCounter
alaMRPDomainMRCRxLinkDownCounter
alaMRPDomainMRC TxLinkDownCounter
alaMRPDomainMRCDropLinkDownCounter
alaMRPDomainMRARxTestMgrNAckCounter
alaMRPDomainMRATxTestMgrNAckCounter
alaMRPDomainMRARxDropTestMgrNAckCounter
alaMRPDomainMRARxTestPropagateCounter
alaMRPDomainMRATxTestPropagateCounter
alaMRPDomainMRARxDropTestPropagateCounter
alaMRPDomainMRARxErrorFrameCounter
alaMRPDomainMIMTopChangeCounter
alaMRPDomainMIMRxTopChangeCounter
alaMRPDomainMIMRxTestDefaultCounter
alaMRPDomainMIMTxTestDefaultCounter
alaMRPDomainMIMRxLinkStatusPollCounter
alaMRPDomainMIMITxLinkStatusPollCounter
alaMRPDomainMICRxLinkUpCounter
alaMRPDomainMICRxLinkDownCounter
alaMRPDomainMIC RxLinkUpCounter
alaMRPDomainMICTxLinkUpCounter
alaMRPDomainMICTxLinkDownCounter
**show mrp interconnect**

Displays the MRP interconnection configuration information for a specific interconnection ID or name.

```plaintext
show mrp [interconnect [{interconnect_id | name name}]] [detail] [ring-port] [counters]
```

### Syntax Definitions

- **interconnect_id**: The interconnection identifier unique in the switch. When specified, displays the MRP interconnection configuration for a MRP interconnect ID.
- **name**: An unique name for the redundant interconnection of MRP rings. When specified, displays the MRP interconnection configuration for a MRP interconnect name.
- **counters**: Display the counters for a specific interconnection ID or name.
- **detail**: Display the MRP interconnection configuration in detail for a specific interconnection ID or name.
- **ring-port**: Display the ring ports belonging to a specific interconnection ID or name.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```plaintext
-> show mrp interconnect 1
Interconnection
ID    Port   Mode  Status  State  Role  VLAN Recovery time(ms)
--------+--------+--------+----------+--------+-------+-----------------+
1      1/1/2 LC Disable Open Manager 50 500

LC - Link-Check, RC - Ring-Check
```
show mrp interconnect detail
Interconnection ID: 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Port state</th>
<th>Mode</th>
<th>Status</th>
<th>VLAN</th>
<th>time(ms)</th>
<th>STM State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/5</td>
<td>Blocked</td>
<td>LC</td>
<td>Enabled</td>
<td>Close</td>
<td>15</td>
<td>200</td>
</tr>
</tbody>
</table>

Last State Change: Tuesday, November 16, 2021, 09h:50m:39s, 855
System Up Time: Tuesday, November 16, 2021, 09h:50m:16s
Interconnection Open Count: 1
Interconnection own MRM MAC: 2c:fa:a2:bb:1c:49
Interconnection NAME: INTERCONNECTION-1
Interconnection peer UUID: 0xffffffff-ffff-ffff-ffff-fffffffffffffffe
Error: 

MIC:
show mrp interconnect detail
Interconnection ID: 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Port state</th>
<th>Mode</th>
<th>Status</th>
<th>VLAN</th>
<th>time(ms)</th>
<th>STM State</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1/7</td>
<td>Forwarding</td>
<td>LC</td>
<td>Enabled</td>
<td>Undefined</td>
<td>15</td>
<td>200</td>
</tr>
</tbody>
</table>

Interconnection own MRM MAC: 2c:fa:a2:bb:1c:49
Interconnection NAME: INTERCONNECTION-1
Interconnection peer UUID: 0xffffffff-ffff-ffff-ffff-fffffffffffffffe

show mrp interconnect 1 ring-port

Interconnection Port Status Port mac
ID Status
1 Enable 1/1/2 Forwarding 00:d0:95:00:00:dd

show mrp interconnect counters
Domain Id: 1
In-Port1: 2/1/3

<table>
<thead>
<tr>
<th>Type</th>
<th>Tx</th>
<th>Rx</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>InStatus Poll</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>InTopology Change</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>InLink Up</td>
<td>19</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>InLink Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

RPort1: 0/1

<table>
<thead>
<tr>
<th>Type</th>
<th>Tx</th>
<th>Rx</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>InStatus Poll</td>
<td>13</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>InTopology Change</td>
<td>32</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>InLink Up</td>
<td>19</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>InLink Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RPort2: 0/2

<table>
<thead>
<tr>
<th>Type</th>
<th>Tx</th>
<th>Rx</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>InStatus Poll</td>
<td>13</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>InTopology Change</td>
<td>32</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>InLink Up</td>
<td>19</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>InLink Down</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Error</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

output definitions

ID
A unique interconnection ID that represents the MRP ring.

Port
The port number.

Port State
Operational state of the interconnection port.
Disabled - indicates that all frames are dropped.
Blocked - indicates that all frames are dropped except
- MRP Interconnection topology change frames,
- MRP Interconnection test frames,
- MRP Interconnection link change frames,
- MRP Interconnection link status poll frames,
- frames from other protocols that also define to pass blocked
  ports.
Forwarding- indicates that all frames are passed through according to
the forwarding behavior of IEEE 802.1D.
NotConnected - indicates that the port has no link.

Mode
Specifies the role of the node.
Undefined- signals that the interconnection mode is neither set to LC
mode nor to RC mode.
LC - indicates that the interconnection mode is set to LC mode.
RC - indicates that the interconnection mode is set to RC mode.

Status
Administrative status of the MRP ring.

Config State
Operational status of the MRP interconnection entity.

Operational Role
The operational role of an MRP interconnection entity per media
redundancy interconnection domain.

Recovery Role
The recovery role of an MRP interconnection entity per media
redundancy interconnection domain.

VLAN
The service VLAN for sending MRP Interconnection frames.

Time (ms)
The maximum recovery time of a ring in milliseconds.

STM State
The protocol machine state.

Last State Change
Timeticks since last change of mrpInterconnectionState to
interconnOpen.

System Up Time
The time of MRP configuration since the last system reboot.

Interconnection Open Count
Counter for MRP Interconnection state changes to interconnOpen.

Interconnection own MRM MAC
The device MAC address of the devices ring manager (MRM).

Elected MIM MAC
The switch MAC address of the elected MIM.

Interconnection NAME
A unique interconnection name that represents the MRP ring.
Release History

Release 8.9R1; command introduced.

Related Commands

**mrp inter connect**

Configures the MRP ring parameters like interconnection index, interconnection ports, admin-role, mode, and recovery time.

**show mrp**

Displays the MRP configuration information.

MIB Objects

- mrpInterconnectionID
- mrpInterconnectionName
- mrpInterconnectionPort
- mrpInterconnectionPortState
- mrpInterconnectionVlanId
- mrpInterconnectionMode
- mrpInterconnectionAdminRole
- mrpInterconnectionOperRole
- mrpInterconnectionState
- mrpInterconnectionError
- mrpInterconnectionOpenCount
- mrpInterconnectionLastOpenChange
- mrpInterconnectionOwnMRMMAC
- mrpInterconnectionPeerRingDomainUUID
- alaMRPInterconnectionAdminState
- alaMRPInterconnectionRecoveryTime

**Interconnection peer UUID**
The domain UUID of the ring the interconnection peer's, connected to the devices interlink port, ring.

**Error**
Displays the reason when the switch cannot reach to the desired administrative state.
clear mrp

Clears the counters for a ring or all the rings in the system.

clear mrp [domain [{id | name name | uuid uuid}] [counters]

Syntax Definitions

id The domain identifier unique in the switch.
name The domain name.
uuid The unique 16 hexadecimal domain ID.

Defaults

This command can be used to clear the counters for a particular domain ID, domain name, UUID.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> clear mrp domain 1 counters

Release History

Release 8.7R2; command introduced.

Related Commands

show mrp Displays the MRP configuration information.
MIB Objects

alaMRPRingPortIfIndex
alaMRPDomainMRPRxTopChangeCounter
alaMRPDomainMRPTxTopChangeCounter
alaMRPDomainMRRxDropTopChangeCounter
alaMRPDomainMRPTestDefaultCounter
alaMRPDomainMRPTxTestDefaultCounter
alaMRPDomainMRRxTestDefaultCounter
alaMRPDomainMRRxLinkUpCounter
alaMRPDomainMRCTxLinkUpCounter
alaMRPDomainMRCDropLinkUpCounter
alaMRPDomainMRRxLinkDownCounter
alaMRPDomainMRCTxLinkDownCounter
alaMRPDomainMRCDropLinkDownCounter
alaMRPDomainMRARxTestMgrNAckCounter
alaMRPDomainMRATxTestMgrNAckCounter
alaMRPDomainMRARxTestPropagateCounter
alaMRPDomainMRATxTestPropagateCounter
alaMRPDomainMRADropTestPropagateCounter
alaMRPDomainMRADropCounter
alaMRPDomainMRARxErrorFrameCounter
clear mrp interconnect

Clears the counters for a ring or all the rings in the system.

clear mrp interconnect [interconnect_id | [counters]]

Syntax Definitions

interconnect_id

The interconnection identifier unique in the switch.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> clear mrp interconnect 1 counters

Release History

Release 8.9R1; command introduced.

Related Commands

show mrp

Displays the MRP configuration information.

MIB Objects

- alaMRPRingPortIfIndex
- alaMRPDomainErrorFrameCounter
- alaMRPInterconnectionMIMTxTopChangeCounter
- alaMRPInterconnectionMIMRxTopChangeCounter
- alaMRPInterconnectionMIMRxTestDefaultCounter
- alaMRPInterconnectionMIMTxTestDefaultCounter
- alaMRPInterconnectionMIMRxLinkStatusPollCounter
- alaMRPInterconnectionMIMTxLinkStatusPollCounter
- alaMRPInterconnectionMICRxLinkUpCounter
- alaMRPInterconnectionMICRxLinkDownCounter
alaMRPInterconnectionMICTxLinkUpCounter
alaMRPInterconnectionMICTxLinkDownCounter
clear mrp port

Clears the counters for domain ring ports in the system.

```
clear mrp port {linkagg agg_id | chassis/slot/port} counters
```

### Syntax Definitions

- `agg_id` A link aggregate ID number.
- `chassis` The chassis identifier.
- `slot/port` The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> clear mrp port linkagg 2 counters
```

### Release History

Release 8.7R2; command introduced.

### Related Commands

- `show mrp` Displays the MRP configuration information.
MIB Objects

alaMRPRingPortIfIndex
alaMRPDomainMRMRxTopChangeCounter
alaMRPDomainMRMTxTopChangeCounter
alaMRPDomainMRMDropTopChangeCounter
alaMRPDomainMRMTestDefaultCounter
alaMRPDomainMRMTxTestDefaultCounter
alaMRPDomainMRMDropTestDefaultCounter
alaMRPDomainMRCRxLinkUpCounter
alaMRPDomainMRCTxLinkUpCounter
alaMRPDomainMRCDropLinkUpCounter
alaMRPDomainMRCRxLinkDownCounter
alaMRPDomainMRCTxLinkDownCounter
alaMRPDomainMRCDropLinkDownCounter
alaMRPDomainMRARxTestMgrNAckCounter
alaMRPDomainMRATxTestMgrNAckCounter
alaMRPDomainMRADropTestMgrNAckCounter
alaMRPDomainMRARxTestPropagateCounter
alaMRPDomainMRATxTestPropagateCounter
alaMRPDomainMRADropTestPropagateCounter
alaMRPDomainErrorFrameCounter
16 MVRP Commands

MVRP (Multiple VLAN Registration Protocol) provides a mechanism for maintaining the contents of Dynamic VLAN Registration Entries for each VLAN, and for propagating the information they contain to other Bridges. MVRP uses MRP (Multiple Registration Protocol) as the underlying mechanism, for the maintenance and propagation of the VLAN information.

MVRP acts as an MRP application, sending and receiving MVRP information encapsulated in an Ethernet frame on a specific MAC address. MVRP allows both end stations and Bridges in a Bridged Local Area Network to issue and revoke declarations relating to membership of VLANs.

Filename: ALCATEL-IND1-MVRP-MIB.mib
Module: alcatelIND1MVRPMIB

A summary of the available commands is listed here:

```
mvrp
mvrp port
mvrp linkagg
mvrp maximum-vlan
mvrp registration
mvrp applicant
mvrp timer join
mvrp timer leave
mvrp timer leaveall
mvrp timer periodic-timer
mvrp periodic-transmission
mvrp restrict-vlan-registration
mvrp restrict-vlan-advertisement
mvrp static-vlan-restrict
show mvrp configuration
show mvrp port
show mvrp linkagg
show mvrp timer
show mvrp statistics
show mvrp last-pdu-origin
show mvrp vlan-restrictions
mvrp clear-statistics
```
mvrp

Enables or disables MVRP globally on the switch.

mvrp {enable | disable}

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables MVRP globally on the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables MVRP globally on the switch.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, MVRP is disabled on the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/V48C8C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Disabling MVRP globally deletes all the MVRP learned VLANs.
- MVRP is supported only when the switch is operating in the flat Spanning Tree mode and it is not supported in the per-VLAN mode.

**Examples**

- `-> mvrp enable`
- `-> mvrp disable`

**Release History**

Release 7.2.1; command introduced.

**Related Commands**

- `show mvrp configuration` Displays the global configuration for MVRP.

**MIB Objects**

- `alaMvrpGlobalStatus`
**mvrp port**

Enables or disables MVRP on specific ports on the switch.

```
mvrp port chassis/slot/port{–port2} {enable | disable}
```

---

**Syntax Definitions**

- **chassis**: The chassis identifier when running in virtual chassis mode.
- **slot/port**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8)
- **enable**: Enables MVRP on a port.
- **disable**: Disables MVRP on a port.

**Defaults**

By default, MVRP is disabled on all the ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP must be enabled globally on the switch.
- When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation.
- MVRP can be enabled only on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (mirroring ports, aggregable ports, VLAN Stacking User ports) do not support MVRP.

**Examples**

```
-> mvrp port 1/2 enable
-> mvrp port 1/2 disable
-> mvrp port 1/1-10 enable
-> mvrp port 1/1-10 disable
```

**Release History**

Release 7.2.1; command introduced.
Related Commands

**show mvrp port**
Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

**show mvrp statistics**
Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

alaMvrpPortConfigTable
alaMvrpPortStatus
**mvrp linkagg**

Enables or disables MVRP on specific aggregates on the switch.

```
mvrp linkagg agg_id[-agg_id2] {enable | disable}
```

**Syntax Definitions**

- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `enable` Enables MVRP for the specified link aggregate ID.
- `disable` Disables MVRP for the specified link aggregate ID.

**Defaults**

By default, MVRP is disabled on all the ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- MVRP can be enabled on switch ports regardless of whether it is globally enabled on the switch. However, for the port to become an active participant in the MVRP operation, MVRP must be enabled globally on the switch.
- When MVRP is globally enabled on the switch and is not enabled on the port, that port is excluded from the MVRP protocol operation.
- MVRP can be enabled only on fixed ports, 802.1 Q ports, aggregate ports, and VLAN Stacking Network ports. Other ports (mirroring ports, aggregable ports, mobile ports, VPLS Access ports, VLAN Stacking User ports) do not support MVRP.
- To use the `agg_id` parameter, the link aggregate group must be created.

**Examples**

- `-> mvrp linkagg 10 enable`
- `-> mvrp linkagg 10 disable`
- `-> mvrp linkagg 2-5 enable`
- `-> mvrp linkagg 1-5 disable`
**Release History**

Release 7.2.1; command introduced.

**Related Commands**

- **show mvrp port**
  Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

- **show mvrp statistics**
  Displays the MVRP statistics for all the ports, aggregates, or specific ports.

**MIB Objects**

alaMvrpPortConfigTable
alaMvrpPortStatus
**mvrp maximum-vlan**

Configures the maximum number of dynamic VLANs that can be created by MVRP.

```
mvrp maximum-vlan vlan_limit
```

### Syntax Definitions

- `vlan_limit` - The maximum number of VLANs to be created by MVRP. The valid range is 32–4094.

### Defaults

The default value is 256.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command can be used even when MVRP is not enabled on the switch. However, MVRP must be enabled on the switch for creating dynamic VLANs.
- If the VLAN limit to be set is less than the current number of dynamically learned VLANs, then the new configuration takes effect only after the MVRP is disabled and re-enabled on the switch. The VLANs learned earlier are retained if this operation is not performed.

### Examples

```
-> mvrp maximum-vlan 100
```

### Release History

Release 7.2.1; command introduced.

### Related Commands

- `show mvrp configuration` - Displays the global configuration for MVRP.
- `show mvrp vlan-restrictions` - Displays the list of VLANs learned through MVRP and their details.

### MIB Objects

- `alaMvrpMaxVlanLimit`
**mvrp registration**

Configures the MVRP registration mode for specific ports or aggregates.

```
mvrp {port chassis/slot/port[- port2] | linkagg agg_id[-agg_id2]} registration {normal | fixed | forbidden}
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.
- **slot/port**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **normal**
  - Specifies that both registration and de-registration of VLANs are allowed. VLANs can be mapped either dynamically (through MVRP) or statically (through management application) on such a port.
- **fixed**
  - Specifies that only static mapping of VLANs is allowed on the port but de-registration of previously created dynamic or static VLANs is not allowed.
- **forbidden**
  - Specifies that dynamic VLAN registration or de-registration is not allowed on the port. Any dynamic VLANs created earlier is de-registered.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>fixed</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

To use the `agg_id` parameter, the link aggregate group must be created and enabled.

### Examples

- `mvrp port 1/2 registration forbidden`
- `mvrp port 1/5 registration normal`
- `mvrp linkagg 10 registration fixed`
-> mvrp linkagg 20 registration forbidden
-> mvrp port 2/5-10 registration normal

**Release History**

Release 7.2.1; command introduced.

**Related Commands**

- **show mvrp port** Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
- **show mvrp linkagg** Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

**MIB Objects**

- **alaMvrpPortConfigTable**
- **alaMvrpPortConfigRegistrarMode**
mvrp applicant

Configures the applicant mode of specific ports on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.

```
mvrp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} applicant {participant | non-participant | active}
```

Syntax Definitions

- `chassis` The chassis identifier.
- `slot/port` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `participant` Specifies that MVRP PDU exchanges are only allowed when the port is in the STP forwarding state.
- `non-participant` Specifies that MVRP PDU’s are not sent in this mode and PDU’s received are processed and learning happens as expected.
- `active` Specifies that MVRP PDU exchanges are allowed when the port is in the STP forwarding state or STP blocking state. This is applicable for both advertisement and registration.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>participant</td>
<td>non-participant</td>
</tr>
<tr>
<td>active</td>
<td>active</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use the `agg_id` parameter, the link aggregate group must be created and enabled.

Examples

- `mvrp port 1/2 applicant active`
- `mvrp port 1/3 applicant participant`
- `mvrp port 1/4 applicant non-participant`
-> mvrp linkagg 10 applicant active
-> mvrp linkagg 15 applicant participant
-> mvrp linkagg 20 applicant non-participant

**Release History**

Release 7.2.1; command introduced.

**Related Commands**

- **show mvrp port**
  Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

- **show mvrp linkagg**
  Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

**MIB Objects**

- **alaMvrpPortConfigTable**
  - **alaMvrpPortConfigApplicantMode**
mvrp timer join

Specifies the join time interval between transmit opportunities for the dynamically registering VLANs on the switch.

\[\text{mvrp} \{\text{port chassis/slot/port[–port2]} | \text{linkagg agg_id[–agg_id2]}\} \text{ timer join timer_value}\]

**Syntax Definitions**

- **chassis**
  - The chassis identifier.
- **slot/port**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[–agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **timer_value**
  - Specifies the value of the join timer in milliseconds. The valid range is 250 milliseconds to 1073741773 milliseconds.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>timer-value</td>
<td>600 milliseconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- To use the `agg_id` parameter, the link aggregate group must be created and enabled.

**Examples**

- `mvrp port 1/2 timer join 600`
- `mvrp port 1/2-12 timer join 600`
- `mvrp linkagg 3 timer join 600`
- `mvrp linkagg 3-6 timer join 600`

**Release History**

Release 7.2.1; command introduced.
Related Commands

- **show mvrp timer**
  Displays the timer values configured for all the ports or a specific port.

- **show mvrp port**
  Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

- `alaMvrpPortConfigTable`
  - `alaMvrpPortConfigJoinTimer`
  - `alaMvrpPortConfigLeaveTimer`
  - `alaMvrpPortConfigLeaveAllTimer`
  - `alaMvrpPortConfigPeriodicTimer`
**mvrp timer leave**

Specifies the period of time that the switch has to wait in the Leave state before changing to the unregistered state.

```
/mvrp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} timer leave timer_value
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **timer-value**
  - Specifies the value of the Leave Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>timer_value</td>
<td>1800</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.

- Leave timer value must be greater than or equal to twice the Join timer value, plus six times the timer resolution (16.66 milliseconds). Leave timer must be at least be greater than twice the join timer plus100 milliseconds.

- To use the `agg_id` parameter, the link aggregate group must be created and enabled.

### Examples

```
-> mvrp port 1/2 timer leave 1800
-> mvrp port 1/2-12 timer leave 1800
-> mvrp linkagg 3 timer leave 1800
-> mvrp linkagg 3-6 timer leave 1800
```
**Release History**

Release 7.2.1; command introduced.

**Related Commands**

- `show mvrp timer` Displays the timer values configured for all the ports or a specific port.
- `show mvrp port` Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

**MIB Objects**

alaMvrpPortConfigTable
  - `alaMvrpPortConfigJoinTimer`
  - `alaMvrpPortConfigLeaveTimer`
  - `alaMvrpPortConfigLeaveAllTimer`
  - `alaMvrpPortConfigPeriodicTime`
**mvrp timer leaveall**

Specifies the frequency with which the LeaveAll messages are communicated.

```
mvrp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} timer leaveall timer_value
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- **timer_value**: Specifies the value of the LeaveAll Timer in milliseconds. The valid range is 750 milliseconds to 2147483647 milliseconds.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>timer-value</td>
<td>30000 milliseconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.
- LeaveAll timer value must be greater than or equal to the Leave timer value. It is recommended to have the leaveall timer 15 times greater than the leave timer.
- To use the `agg_id` parameter, the link aggregate group must be created and enabled.

**Examples**

- `-> mvrp port 1/2 timer leaveall 30000`
- `-> mvrp port 1/2-12 timer leaveall 30000`
- `-> mvrp linkagg 3 timer leaveall 30000`
- `-> mvrp linkagg 3-6 timer leaveall 30000`

**Release History**
Release 7.2.1; command introduced.

**Related Commands**

- `show mvrp timer` Displays the timer values configured for all the ports or a specific port.
- `show mvrp port` Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

**MIB Objects**

alaMvrpPortConfigTable
  alaMvrpPortConfigJoinTimer
  alaMvrpPortConfigLeaveTimer
  alaMvrpPortConfigLeaveAllTimer
  alaMvrpPortConfigPeriodicTimer
**mvrp timer periodic-timer**

Specifies the MVRP periodic-timer time interval for the dynamically registering VLANs on the switch.

```
mvrp {port chassis/slot/port[– port2] | linkagg agg_id[-agg_id2]} timer periodic-timer timer_value
```

### Syntax Definitions

- `chassis`  
  The chassis identifier.
- `slot/port`  
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]`  
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `timer_value`  
  Specifies the value of the Periodic Timer in seconds. The valid range is between 1 to 2147483647 milliseconds.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>timer-value</td>
<td>1 second</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900/6900/6900</th>
<th>6900/6900/6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use default timer settings unless there is a compelling reason to change the settings. Modifying timers to inappropriate values can cause an imbalance in the operation of MVRP.

- To use the `agg_id` parameter, the link aggregate group must be created and enabled.

### Examples

```
-> mvrp port 1/2 timer periodic-timer 1
-> mvrp port 1/2 timer periodic-timer 1
-> mvrp linkagg 3 timer periodic-timer 1
-> mvrp linkagg 3-6 timer periodic-timer 1
```

### Release History

Release 7.2.1; command introduced.
Related Commands

- **show mvrp timer**
  Displays the timer values configured for all the ports or a specific port.
- **show mvrp port**
  Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

- **alaMvrpPortConfigTable**
- **alaMvrpPortConfigJoinTimer**
- **alaMvrpPortConfigLeaveTimer**
- **alaMvrpPortConfigLeaveAllTimer**
- **alaMvrpPortConfigPeriodicTimer**
mvrp periodic-transmission

Enables the periodic transmission status on a port or aggregate of ports.

```
mvrp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} periodic-transmission {enable | disable}
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `enable` Enables periodic transmission status on a port.
- `disable` Disables periodic transmission status on a port.

**Defaults**

By default, periodic-transmission status is disabled on all the ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use the `agg_id` parameter, the link aggregate group must be created and enabled.

**Examples**

- `-> mvrp port 1/2 periodic-transmission enable`
- `-> mvrp port 1/2 periodic-transmission disable`
- `-> mvrp linkagg 10 periodic-transmission enable`
- `-> mvrp linkagg 10 periodic-transmission disable`

**Release History**

Release 7.2.1; command introduced.
Related Commands

**show mvrp port**
Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

**show mvrp linkagg**
Displays the MVRP configurations for all link aggregates, including timer values, registration and applicant modes.

MIB Objects

alaMvrpPortConfigTable

alaMvrpPortConfigPeriodicTransmissionStatus
mv rp restrict-vlan-registration

Restricts MVRP processing from dynamically registering the specified VLAN or VLANs on the switch.

```plaintext
mv rp [port chassis/slot/port [-port2] | linkagg agg_id[-agg_id2]] restrict-vlan-registration vlan vlan_list
```

```plaintext
no mv rp [port chassis/slot/port [-port2] | linkagg agg_id[-agg_id2]] restrict-vlan-registration vlan vlan_list
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `vlan_list` The VLAN ID or the VLAN ID range (for example, 1-10).

**Defaults**

By default, MVRP dynamic VLAN registrations are not restricted.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to allow registration of dynamic VLAN IDs through MVRP processing.
- If the specified VLAN exists on the switch, the VLAN is mapped to the receiving port.
- To use the `agg_id` parameter, the link aggregate group must be created and enabled.

**Examples**

- `mv rp port 1/2 restrict-vlan-registration vlan 5`
- `no mv rp port 1/2 restrict-vlan-registration vlan 5`
- `mv rp linkagg 10 restrict-vlan-registration vlan 6-10`
- `no mv rp port 3/1 restrict-vlan-registration vlan 6-10`
**Release History**

Release 7.2.1; command introduced.

**Related Commands**

*show mvrp port* Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

*show mvrp linkagg* Displays the MVRP configurations for all link aggregates, including timer values, registration and applicant modes.

**MIB Objects**

alaMvrpPortRestrictVlanConfigTable

alaMvrpPortRestrictRowStatus

alaMvrpPortRestrictVlanAttributeType

alaMvrpPortRestrictVlanID
mvrp restrict-vlan-advertisement

Restricts the advertisement of VLANs on a specific port or an aggregate of ports.

```
mvrp [port chassis/slot/port|linkagg agg_id]-agg_id2] restrict-vlan-advertisement vlan vlan_list

no mvrp [port chassis/slot/port|linkagg agg_id]-agg_id2] restrict-vlan-advertisement vlan vlan_list
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id|agg_id2` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `vlan_list` The list of VLAN IDs or the VLAN ID range (for example, 1-10).

**Defaults**

By default, MVRP VLAN advertisement is not restricted.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command affects the MVRP processing only if the applicant mode is set to participant or active.
- Use the `no` form of this command to allow the propagation of VLANs.
- To use the `agg_id` parameter, the link aggregate group must be created and enabled.

**Examples**

```
-> mvrp port 1/2 restrict-vlan-advertisement vlan 5
-> no mvrp port 1/2 restrict-vlan-advertisement vlan 5
-> mvrp linkagg 10 restrict-vlan-advertisement vlan 6-10
-> no mvrp port 1/2 restrict-vlan-advertisement vlan 6-10
-> no mvrp port 1/1-2 restrict-vlan-advertisement vlan 6-10
```

**Release History**
Release 7.2.1; command introduced.

**Related Commands**

- **mvrp applicant** Configures the applicant mode of specific ports on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.

- **mvrp timer join** Configures the applicant mode of specific link aggregates on the switch. The applicant mode determines whether MVRP PDU exchanges are allowed on a port depending on the Spanning Tree state of the port.

- **show mvrp port** Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

- **show mvrp linkagg** Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

**MIB Objects**

alaMvrpPortRestrictVlanConfigTable
- alaMvrpPortRestrictRowStatus
- alaMvrpPortRestrictVlanAttributeType
- alaMvrpPortRestrictVlanID
mvrp static-vlan-restrict

Restricts a port from becoming a member of a statically created VLAN or a range of VLANs.

```
mvrp {linkagg agg_id[-agg_id2] | port chassis/slot/port[-port2]} static-vlan-restrict vlan vlan_list
```

```
no mvrp {linkagg agg_id[-agg_id2] | port chassis/slot/port[-port2]} static-vlan-restrict vlan vlan_list
```

### Syntax Definitions

- `chassis`  
The chassis identifier.
- `slot/port`  
The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]`  
The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `vlan_list`  
The list of VLAN IDs or the VLAN ID range (for example, 1-10).

### Defaults

By default, ports are assigned to the static VLAN based on MVRP PDU processing.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command applies only to static VLANs and does not apply to dynamic VLANs.
- Use the `no` form of this command to set the specified port and VLAN to the default value.

### Examples

- `-> mvrp port 1/2 static-vlan-restrict vlan 5`
- `-> no mvrp port 1/2 static-vlan-restrict vlan 5`
- `-> mvrp port 1/2 static-vlan-restrict vlan 6-9`
- `-> no mvrp port 1/2 static-vlan-restrict vlan 6-9`
- `-> mvrp linkagg 3 static-vlan-restrict vlan 4-5`
- `-> no mvrp linkagg 3 static-vlan-restrict aggregate vlan 4-5`

### Release History

Release 7.2.1; command introduced.
**Related Commands**

- `show mvrp port`  
  Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

- `show mvrp linkagg`  
  Displays the MVRP configurations for all the link aggregates, including timer values, registration and applicant modes.

**MIB Objects**

- `alaMvrpPortRestrictVlanConfigTable`
  - `alaMvrpPortRestrictRowStatus`
  - `alaMvrpPortRestrictVlanAttributeType`
  - `alaMvrpPortRestrictVlanID`
  - `alaMvrpPortConfigRegistrationToStaticVlan`
  - `alaMvrpPortConfigRegistrationToStaticVlanLearn`
  - `alaMvrpPortConfigRegistrationToStaticVlanRestrict`
show mvrp configuration

Displays the global configuration for MVRP.

**show mvrp configuration**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show mvrp configuration
MVRP Enabled : yes,
Maximum VLAN Limit : 256
```

**output definitions**

<table>
<thead>
<tr>
<th>MVRP Enabled</th>
<th>Indicates whether MVRP is globally enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum VLAN Limit</td>
<td>The maximum number of VLANs that can be learned by MVRP in the system.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.2.1; command introduced.
Related Commands

**mvrp**
Enables or disables MVRP globally on the switch.

**mvrp maximum-vlan**
Configures the maximum number of dynamic VLANs that can be created by MVRP.

MIB Objects

- alaMvrpGlobalStatus
- alaMvrpMaxVlanLimit
**show mvrp port**

Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

`show mvrp port [chassis/slot/port[-port2]] [enable | disable]`

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **enable**: To display only the enabled ports.
- **disable**: To display only the disabled ports.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show mvrp port enable

Port   Join      Leave LeaveAll Periodic  Registration  Applicant    Periodic Tx
Timer   Timer  Timer    Timer    Mode        Mode        Status
          (msec) (msec) (msec)   (sec)       (msec)   (sec)        
1/1 600 1800 30000 2 fixed       active      enabled
1/2 600 1800 30000 2 fixed       active      enabled
1/7 600 1800 30000 2 fixed       active      enabled
1/8 600 1800 30000 2 fixed       active      enabled
2/24 600 1800 30000 2 fixed       active      enabled
```

```
-> show mvrp port disable

```

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 16-30
### MVRP Commands

#### show mvrp port

<table>
<thead>
<tr>
<th>Port</th>
<th>Join Timer (msec)</th>
<th>Leave Timer (msec)</th>
<th>LeaveAll Timer (msec)</th>
<th>Periodic Registration Timer (sec)</th>
<th>Applicant Mode</th>
<th>Periodic Tx Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/9</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>2</td>
<td>fixed</td>
<td>active</td>
</tr>
<tr>
<td>1/10</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>2</td>
<td>fixed</td>
<td>active</td>
</tr>
<tr>
<td>2/1</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>2</td>
<td>fixed</td>
<td>active</td>
</tr>
<tr>
<td>2/2</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>2</td>
<td>fixed</td>
<td>active</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/24</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>2</td>
<td>fixed</td>
<td>active</td>
</tr>
</tbody>
</table>

-> show mvrp port

<table>
<thead>
<tr>
<th>Port Status</th>
<th>Join Timer (msec)</th>
<th>Leave Timer (msec)</th>
<th>LeaveAll Timer (msec)</th>
<th>Periodic Registration Timer (sec)</th>
<th>Applicant Mode</th>
<th>Periodic Tx Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>disabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>participant</td>
</tr>
<tr>
<td>1/2</td>
<td>enabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>participant</td>
</tr>
<tr>
<td>1/3</td>
<td>enabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>active</td>
</tr>
<tr>
<td>1/4</td>
<td>enabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>active</td>
</tr>
<tr>
<td>2/24</td>
<td>enabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>active</td>
</tr>
</tbody>
</table>

-> show mvrp port 1/1-3

<table>
<thead>
<tr>
<th>Port Status</th>
<th>Join Timer (msec)</th>
<th>Leave Timer (msec)</th>
<th>LeaveAll Timer (msec)</th>
<th>Periodic Registration Timer (sec)</th>
<th>Applicant Mode</th>
<th>Periodic Tx Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>disabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>participant</td>
</tr>
<tr>
<td>1/2</td>
<td>enabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>participant</td>
</tr>
<tr>
<td>1/3</td>
<td>enabled</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>fixed</td>
<td>active</td>
</tr>
</tbody>
</table>

-> show mvrp port 1/1

MVRP Enabled : no,
Registrar Mode : normal,
Applicant Mode : participant,
Join Timer (msec) : 600,
Leave Timer (msec) : 1800,
LeaveAll Timer (msec) : 30000,
Periodic Timer (sec) : 1,
Periodic Tx Status : enabled

-> show mvrp port 1/1 enable

ERROR: MVRP is disabled on port 1/1

### Output Definitions

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Displays the slot and port number.</td>
</tr>
<tr>
<td>Join Timer</td>
<td>Displays the value of Join Timer in milliseconds.</td>
</tr>
<tr>
<td>Leave Timer</td>
<td>Displays the value of the Leave Timer in milliseconds.</td>
</tr>
<tr>
<td>LeaveAll Timer</td>
<td>Displays the value of the LeaveAll Timer in milliseconds.</td>
</tr>
<tr>
<td>Periodic Timer</td>
<td>Displays the value of the Periodic Timer in seconds.</td>
</tr>
<tr>
<td>Periodic Tx Status</td>
<td>The transmission status of MVRP, enable or disable.</td>
</tr>
</tbody>
</table>
Release History

Release 7.2.1; command introduced.

Related Commands

mvrp port
Enables or disables MVRP on specific ports on the switch.

mvrp
Configures VLAN dynamic registration mode to MVRP and deletes all static configuration of previous mode along with the dynamic data.

MIB Objects

alaMvrpPortConfigTable
  alaMvrpPortStatus
  alaMvrpPortConfigRegistrarMode
  alaMvrpPortConfigApplicantMode
  alaMvrpPortConfigJoinTimer
  alaMvrpPortConfigLeaveTimer
  alaMvrpPortConfigLeaveAllTimer
  alaMvrpPortConfigPeriodicTimer
  alaMvrpPortConfigPeriodicTransmissionStatus
show mvrp linkagg

Displays the MVRP configurations for linkaggs, including timer values, registration and applicant modes.

\texttt{show mvrp linkagg [agg_id]-[agg_id2]} \texttt{[enabled | disabled]}

\textbf{Syntax Definitions}

- \texttt{agg_id} - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- \texttt{enabled} - To display only the enabled ports.
- \texttt{disabled} - To display only the disabled ports.

\textbf{Defaults}

N/A

\textbf{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\textbf{Usage Guidelines}

N/A

\textbf{Examples}

\texttt{-> show mvrp linkagg 1-3}

\begin{tabular}{|c|c|c|c|c|c|c|c|c|c|}
\hline
Port Status & Join Timer (msec) & Leave Timer (msec) & LeaveAll Timer (msec) & Periodic Timer (sec) & Registration Mode & Applicant Mode & Periodic Tx Status \\
\hline
0/1 enabled & 600 & 1800 & 30000 & 2 & fixed & participant & enabled \\
0/2 enabled & 600 & 1800 & 30000 & 2 & fixed & participant & enabled \\
0/3 enabled & 600 & 1800 & 30000 & 2 & fixed & participant & enabled \\
\hline
\end{tabular}

\texttt{-> show mvrp linkagg 1}

MVRP Enabled : yes, 
Registrar Mode : normal, 
Applicant Mode : participant, 
Join Timer (msec) : 600, 
Leave Timer (msec) : 1800, 
LeaveAll Timer (msec) : 30000, 
Periodic Timer (sec) : 1, 
Periodic Tx Status: enabled
-> show mvrp linkagg 1 disable
ERROR: MVRP is enabled on linkagg 0/1

**Note.** In the command output shown below, the MVRP status is not displayed as the command is only for enabled ports and link aggregates.

-> show mvrp linkagg 10 enable
Registrar Mode : normal,
Applicant Mode : participant,
Join Timer (msec) : 600,
Leave Timer (msec) : 1800,
LeaveAll Timer (msec) : 30000,
Periodic Timer (sec) : 1,
Periodic Tx status : disabled

**output definitions**

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the slot/port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Timer</td>
<td>Displays the value of Join Timer in milliseconds.</td>
</tr>
<tr>
<td>Leave Timer</td>
<td>Displays the value of the Leave Timer in milliseconds.</td>
</tr>
<tr>
<td>LeaveAll Timer</td>
<td>Displays the value of the LeaveAll Timer in milliseconds.</td>
</tr>
<tr>
<td>Periodic Timer</td>
<td>Displays the value of the Periodic Timer in seconds.</td>
</tr>
<tr>
<td>Periodic Tx Status</td>
<td>The transmission status of MVRP, enable or disable</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.2.1; command introduced.

**Related Commands**

**mvrp port**

Enables or disables MVRP on specific ports on the switch.

**MIB Objects**

alaMvrpPortConfigTable
  alaMvrpPortStatus
  alaMvrpPortConfigRegistrarMode
  alaMvrpPortConfigApplicantMode
  alaMvrpPortConfigJoinTimer
  alaMvrpPortConfigLeaveTimer
  alaMvrpPortConfigLeaveAllTimer
  alaMvrpPortConfigPeriodicTimer
  alaMvrpPortConfigPeriodicTransmissionStatus
show mvrp timer

Displays the timer values configured for all the ports or a specific port.

`show mvrp [port chassis/slot/port|–port2] | linkagg agg_id[-agg_id2]] timer {join | leave | leaveall | periodic-timer}`

### Syntax Definitions

- **chassis**
  The chassis identifier when running in virtual chassis mode.

- **slot/port**
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **join**
  To display only the join timer.

- **leave**
  To display only the leave timer.

- **leaveall**
  To display only the leaveall timer.

- **periodic-timer**
  To display only the periodic-timer.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `join`, `leave`, `leaveall`, or `periodic-timer` parameter with this command to view the specific timer values configured on all the ports.

- Use the `agg_id` or `slot/port` parameter with this command to display the timer values configured for a specific port.

### Examples

```
-> show mvrp timer
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Join Timer (msec)</th>
<th>Leave Timer (msec)</th>
<th>LeaveAll Timer (sec)</th>
<th>Periodic Timer (msec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>2</td>
</tr>
<tr>
<td>1/2</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>5</td>
</tr>
</tbody>
</table>
show mvrp timer

<table>
<thead>
<tr>
<th>Port</th>
<th>Join Timer</th>
<th>Leave Timer</th>
<th>LeaveAll Timer</th>
<th>Periodic-Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>1</td>
</tr>
<tr>
<td>1/2</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>1</td>
</tr>
<tr>
<td>1/3</td>
<td>600</td>
<td>1800</td>
<td>30000</td>
<td>1</td>
</tr>
</tbody>
</table>

Legend: All timer values are in milliseconds

Port | LeaveAll Timer
--------+----------------
1/1    1800
1/2    1800
1/3    1800

Port | Periodic Timer
--------+----------------
1/1    1
1/2    1
1/3    1
show mvrp timer

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the slot/port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Timer</td>
<td>Displays the value of Join Timer in milliseconds.</td>
</tr>
<tr>
<td>Leave Timer</td>
<td>Displays the value of the Leave Timer in milliseconds.</td>
</tr>
<tr>
<td>LeaveAll Timer</td>
<td>Displays the value of the LeaveAll Timer in milliseconds.</td>
</tr>
<tr>
<td>Periodic Timer</td>
<td>Displays the value of the Periodic Timer in seconds.</td>
</tr>
</tbody>
</table>

Release History

Release 7.2.1; command introduced.

Related Commands

- **mvrp timer join**: Specifies the join time interval between transmit opportunities for the dynamically registering VLANs on the switch.
- **mvrp timer leave**: Specifies the period of time that the switch has to wait in the Leave state before changing to the unregistered state.
- **mvrp timer leaveall**: Specifies the frequency with which the LeaveAll messages are communicated.
- **mvrp timer periodic-timer**: Specifies the MVRP periodic-timer time interval for the dynamically registering VLANs on the switch.
- **show mvrp port**: Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

alaMvrpPortConfigTable
  - alaMvrpPortConfigJoinTimer
  - alaMvrpPortConfigLeaveTimer
  - alaMvrpPortConfigLeaveAllTimer
  - alaMvrpPortConfigPeriodicTimer
show mvrp statistics

Displays the MVRP statistics for all the ports, aggregates, or specific ports.

show mvrp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} statistics

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If no port or link aggregate is specified the MVRP statistics are displayed for all ports.
- Use the **agg_id or slot/port** parameter with this command to display the MVRP statistics for a specific port.

Examples

```bash
-> show mvrp port 1/1/1 statistics
Port 1/1/1:
   New Received       : 0,
   Join In Received   : 1526,
   Join Empty Received: 8290,
   Leave Received     : 0,
   In Received        : 1,
   Empty Received     : 0,
   Leave All Received : 283,
   New Transmitted    : 826,
   Join In Transmitted: 1532,
   Join Empty Transmitted: 39,
   Leave Transmitted  : 0,
   In Transmitted     : 0,
   Empty Transmitted  : 296,
```
MVRP Commands

show mvrp statistics

LeaveAll Transmitted : 23,
Failed Registrations : 0,
Total Mrp PDU Received : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msqs Received : 10100,
Total Mrp Msqs Transmitted : 2693,
Invalid Msqs Received : 0

--> show mvrp statistics

Port 1/1/1:
New Received : 0,
Join In Received : 1526,
Join Empty Received : 8290,
Leave Received : 0,
In Received : 1,
Empty Received : 0,
Leave All Received : 283,
New Transmitted : 826,
Join In Transmitted : 1532,
Join Empty Transmitted : 39,
Leave Transmitted : 0,
In Transmitted : 0,
Empty Transmitted : 296,
LeaveAll Transmitted : 23,
Failed Registrations : 0,
Total Mrp PDU Received : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msqs Received : 10100,
Total Mrp Msqs Transmitted : 2693,
Invalid Msqs Received : 0

Port 1/1/2:
New Received : 0,
Join In Received : 1526,
Join Empty Received : 8290,
Leave Received : 0,
In Received : 1,
Empty Received : 0,
Leave All Received : 283,
New Transmitted : 826,
Join In Transmitted : 1532,
Join Empty Transmitted : 39,
Leave Transmitted : 0,
In Transmitted : 0,
Empty Transmitted : 296,
LeaveAll Transmitted : 23,
Failed Registrations : 0,
Total Mrp PDU Received : 1160,
Total Mrp PDU Transmitted : 957,
Total Mrp Msqs Received : 10100,
Total Mrp Msqs Transmitted : 2693,
Invalid Msqs Received : 0
output definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Received</td>
<td>The number of new MVRP messages received on the switch.</td>
</tr>
<tr>
<td>Join In Received</td>
<td>The number of MVRP Join In messages received on the switch.</td>
</tr>
<tr>
<td>Join Empty Received</td>
<td>The number of MVRP Join Empty messages received on the switch.</td>
</tr>
<tr>
<td>Leave In Received</td>
<td>The number of MVRP Leave In messages received on the switch.</td>
</tr>
<tr>
<td>In Received</td>
<td>The total MVRP messages received on the switch.</td>
</tr>
<tr>
<td>Empty Received</td>
<td>The number of MVRP Empty messages received on the switch.</td>
</tr>
<tr>
<td>Leave All Received</td>
<td>The number of MVRP Leave All messages received on the switch.</td>
</tr>
<tr>
<td>New Transmitted</td>
<td>The number of new MVRP messages sent by the switch.</td>
</tr>
<tr>
<td>Join In Transmitted</td>
<td>The number of MVRP Join In messages sent by the switch.</td>
</tr>
<tr>
<td>Join Empty Transmitted</td>
<td>The number of MVRP Join Empty messages sent by the switch.</td>
</tr>
<tr>
<td>Leave Transmitted</td>
<td>The number of MVRP Leave messages sent by the switch.</td>
</tr>
<tr>
<td>In Transmitted</td>
<td>The number of MVRP In messages sent by the switch.</td>
</tr>
<tr>
<td>Empty Transmitted</td>
<td>The number of MVRP empty messages sent by the switch.</td>
</tr>
<tr>
<td>LeaveAll Transmitted</td>
<td>The number of Leave All messages sent by the switch.</td>
</tr>
<tr>
<td>Failed Registrations</td>
<td>The number of failed registrations.</td>
</tr>
<tr>
<td>Total Mrp PDU Received</td>
<td>The number of total MRP PDUs received by the switch.</td>
</tr>
<tr>
<td>Total Mrp Msgs Received</td>
<td>The number of total MRP messages received by the switch.</td>
</tr>
<tr>
<td>Total Mrp Msgs Transmitted</td>
<td>The number of total MRP messages sent by the switch.</td>
</tr>
<tr>
<td>Invalid Msgs Received</td>
<td>The number of invalid messages received by the switch.</td>
</tr>
</tbody>
</table>

Release History

Release 7.2.1; command introduced.

Related Commands

- `show mvrp configuration` Clears MVRP statistics for all ports, an aggregate of ports, or a specific port.
- `show mvrp port` Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
- `show mvrp linkagg` Displays the MVRP configuration for a specific port or an aggregate of ports.
MIB Objects

alaMvrpPortStatsTable
alaMvrpPortStatsNewReceived
alaMvrpPortStatsJoinInReceived
alaMvrpPortStatsJoinEmptyReceived
alaMvrpPortStatsLeaveReceived
alaMvrpPortStatsInReceived
alaMvrpPortStatsEmptyReceived
alaMvrpPortStatsLeaveAllReceived
alaMvrpPortStatsNewTransmitted
alaMvrpPortStatsJoinInTransmitted
alaMvrpPortStatsJoinEmptyTransmitted
alaMvrpPortStatsLeaveTransmitted
alaMvrpPortStatsInTransmitted
alaMvrpPortStatsEmptyTransmitted
alaMvrpPortStatsLeaveAllTransmitted
alaMvrpPortStatsTotalPDUReceived
alaMvrpPortStatsTotalPDUTransmitted
alaMvrpPortStatsTotalMsgsReceived
alaMvrpPortStatsTotalMsgsTransmitted
alaMvrpPortStatsInvalidMsgsReceived
alaMvrpPortFailedRegistrations
show mvrp last-pdu-origin

Displays the source MAC address of the last MVRP message received on specific ports or aggregates.

show mvrp {port chassis/slot/port|-- port2 | link agg_id[-agg_id2]} last-pdu-origin

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show mvrp port 1/1-3 last-pdu-origin

<table>
<thead>
<tr>
<th>Port</th>
<th>Last PDU Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>00:d0:95:ee:f4:64</td>
</tr>
<tr>
<td>1/2</td>
<td>00:d0:95:ee:f4:65</td>
</tr>
<tr>
<td>1/3</td>
<td>00:d0:95:ee:f4:66</td>
</tr>
</tbody>
</table>

->show mvrp port 1/21 last-pdu-origin

<table>
<thead>
<tr>
<th>Port</th>
<th>Last PDU Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>Displays the slot and port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last PDU origin</td>
<td>The source MAC address of the last PDU message received on the specific port.</td>
</tr>
</tbody>
</table>

Release History

Release 7.2.1; command introduced.

Related Commands

show mvrp linkagg
Displays the MVRP configuration for a specific port or an aggregate of ports.

show mvrp port
Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.

MIB Objects

alaMvrpPortStatsTable
alaMvrpPortLastPduOrigin
show mvrp vlan-restrictions

Displays the VLAN MVRP configuration on a specific port or an aggregate of ports.

`show mvrp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} vlan-restrictions`

**Syntax Definitions**

- `chassis` : The chassis identifier.
- `slot/port` : The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` : The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `agg_id` or `slot/port` parameter with this command to display the MVRP statistics for a specific port.

**Examples**

`-> show mvrp port 1/21 vlan-restrictions`

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Static Registration</th>
<th>Restricted Registration</th>
<th>Restricted Applicant</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LEARN</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>2</td>
<td>LEARN</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>3</td>
<td>LEARN</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>4</td>
<td>LEARN</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>5</td>
<td>LEARN</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>6</td>
<td>LEARN</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>7</td>
<td>LEARN</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>11</td>
<td>RESTRICT</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>12</td>
<td>RESTRICT</td>
<td>FALSE</td>
<td>FALSE</td>
</tr>
<tr>
<td>53</td>
<td>LEARN</td>
<td>TRUE</td>
<td>FALSE</td>
</tr>
<tr>
<td>55</td>
<td>LEARN</td>
<td>FALSE</td>
<td>TRUE</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN ID</td>
<td>The VLAN identification number for a preconfigured VLAN that handles the MVRP traffic for this port.</td>
</tr>
<tr>
<td>Static Registration</td>
<td>Indicates if the port is restricted (RESTRICT) or not restricted (LEARN) from becoming a member of the static VLAN.</td>
</tr>
<tr>
<td>Restricted Registration</td>
<td>Indicates if the VLAN is restricted (TRUE) or not restricted (FALSE) from dynamic registration on the port.</td>
</tr>
<tr>
<td>Restricted Applicant</td>
<td>Indicates if the VLAN is restricted for advertisement from the port (TRUE) or not (FALSE).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.2.1; command introduced.

**Related Commands**

- `show mvrp port` Displays the MVRP configurations for all the ports, including timer values, registration and applicant modes.
- `show mvrp linkagg` Displays the MVRP configuration for a specific port or an aggregate of ports.

**MIB Objects**

- `alaMvrpPortConfigTable`
  - `alaMvrpPortConfigRestrictedRegistrationBitmap`
  - `alaMvrpPortConfigRestrictedApplicantBitmap`
  - `alaMvrpPortConfigRegistrationToStaticVlan`
**mvrp clear-statistics**

Clears MVRP statistics for all the ports, an aggregate of ports, or a specific port.

```
mvrp [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] clear-statistics
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

### Defaults

If no ports are specified, the MVRP statistics are deleted for all the ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `agg_id` or `slot/port` parameter with this command to clear MVRP statistics for a specific port.

### Examples

- `-> mvrp clear-statistics`
- `-> mvrp port 1/2 clear-statistics`
- `-> mvrp linkagg 10 clear-statistics`

### Release History

Release 7.2.1; command introduced.
Related Commands

show mvrp statistics  Displays the MVRP statistics for all the ports, aggregates, or specific ports.

MIB Objects

alaMvrpGlobalClearStats
alaMvrpPortStatsTable
alaMvrpPortStatsClearStats
17 802.1AB Commands

802.1AB is an IEEE standard for exchanging information with neighboring devices and maintaining a database of it. The information is exchanged as an LLDPDU (Link Layer Discovery Protocol Data Unit) in TLV (Time, Length, Value) format. This chapter details configuring and monitoring 802.1AB on a switch.

The OmniSwitch version of 802.1AB complies with the following:

- IEEE 802.1AB-2009 Station and Media Access Control Discovery

MIB information for the 802.1AB commands is as follows:

- **MIB Filename**: LLDP-MIB.mib, LLDP-TC-MIB.mib, LLDP-EXT-DOT1-MIB.mib, LLDP-EXT-DOT3-MIB.mib, LLDP-EXT-MED-MIB.mib
- **MIB V2 Filenames**: LLDP-V2-MIB.mib, LLDP-V2-TC-MIB.mib, LLDP-EXT-DOT1-V2-MIB.mib, LLDP-EXT-DOT3-V2-MIB.mib, LLDP-EXT-MED-MIB.mib

- **Filename**: ALCATEL-IND1-LLDP-MED-MIB.mib
- **Module**: alcatelIND1LLDPMEDMIB
- **Filename**: ALCATEL-IND1-LLDP-TRUST-MIB.mib
- **Module**: alcatelIND1LLDPTRUSTMIB
A summary of available commands is listed here:

- lldp nearest-edge mode
- lldp transmit interval
- lldp transmit hold-multiplier
- lldp reinit delay
- lldp notification interval
- lldp lldpdu
- lldp notification
- lldp network-policy
- lldp med network-policy
- lldp tlv management
- lldp tlv dot1
- lldp tlv dot3
- lldp tlv med
- lldp tlv proprietary
- lldp tlv application
- lldp tlv application priority
- lldp port-id sub-type
- lldp port med-device
- lldp chassis-mac-delimiter
- show lldp statistics
- show lldp local-system
- show lldp local-port
- show lldp local-management-address
- show lldp config
- show lldp network-policy
- show lldp med network-policy
- show lldp remote-system
- show lldp remote-system med
- show lldp remote-system application-tlv
- show lldp remote-system power-via-mdi
- show lldp remote-system power-via-mdi-measurements
- show lldp local-port power-via-mdi
- show lldp local-port power-via-mdi-measurements
- lldp trust-agent
- lldp trust-agent violation-action
- show lldp trusted remote-agent
- show lldp trust-agent

Configuration procedures for 802.1AB are explained in “Configuring 802.1AB,” *OmniSwitch AOS Release 8 Network Configuration Guide.*
**lldp nearest-edge mode**

Enables or disables the nearest-edge mode for the switch. When enabled, the switch will use the LLDP destination MAC address (01:20: DA: 02:01:73) to send LLDPDUs.

```
lldp nearest-edge mode {enable | disable}
```

### Syntax Definitions

- **enable**
  - Enables the nearest-edge mode.
- **disable**
  - Disables the nearest-edge mode.

### Defaults

NA

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The **nearest-edge** MAC address is used in conjunction with the Auto Download Configuration feature to advertise the management VLAN.
- This mode is used to learn the Management VLAN ID from a centralized Remote Configuration management switch.

### Examples

```
-> lldp nearest-edge mode enable
```

### Release History

Release 7.3.4; command introduced.

### Related Commands

- **show lldp local-system**
  - Displays local system information.

### MIB Objects

- **lldpDestMac**
lldp transmit interval

Sets the transmit time interval for LLDPDUs.

**lldp transmit interval seconds**

---

**Syntax Definitions**

```
seconds          The transmit interval between LLDPDUs, in seconds. The valid range is 5 - 32768.
```

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The LLDP protocol must be enabled before using this command.

**Examples**

```
-> lldp transmit interval 40
```

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
Related Commands

**lldp transmit hold-multiplier**  
Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.

**show lldp local-system**  
Displays local system information.

MIB Objects

lldpConfiguration

  lldpV2MessageTxInterval
illdp transmit hold-multiplier

Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.

illdp transmit hold-multiplier num

Syntax Definitions

num The transmit hold multiplier value. The valid range is 2-10.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>4</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The LLDP protocol must be enabled before using this command.
- The Time To Live is a multiple of transmit interval and transmit hold multiplier.

Examples

-> illdp transmit hold-multiplier 6

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
**Related Commands**

- **lldp transmit interval**
  Sets the transmit time interval for LLDPDUs.

- **show lldp local-system**
  Displays local system information.

**MIB Objects**

```plaintext
lldpConfiguration
  lldpV2MessageTxHoldMultiplier
```
**lldp reinit delay**

Sets the time interval that must elapse before the current status of a port is reinitialized after a status change.

`lldp reinit delay seconds`

---

**Syntax Definitions**

`seconds`  The number of seconds to reinitialize the ports status after a status change. The valid range is 1-10.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>2</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The LLDP protocol must be enabled before using this command.

---

**Examples**

`-> lldp reinit delay 4`

---

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
Related Commands

- **lldp transmit interval**
  - Sets the minimum time interval between successive LLDPDUs transmitted.

- **show lldp local-system**
  - Displays local system information.

MIB Objects

- **lldpConfiguration**
  - **lldpV2ReinitDelay**
**lldp notification interval**

Sets the time interval that must elapse before a notification about the local system MIB change is generated.

`lldp notification interval seconds`

---

**Syntax Definitions**

`seconds`

The minimum number of seconds for generating a notification-event. The valid range is 5-3600.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>5</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The LLDP protocol and notification must be enabled before using this command.
- In a specified interval, it is not possible to generate more than one notification-event.

---

**Examples**

```
-> lldp notification interval 25
```

---

**Release History**

- Release 7.1.1; command introduced.
- Release 7.3.1; Version 2 (2009) updates implemented.
**Related Commands**

**lldp notification**  Specifies the switch to control per port notification status about the remote device change.

**show lldp local-system**  Displays local system information.

**MIB Objects**

lldpConfiguration

  lldpV2NotificationInterval
**lldp lldpdu**

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

```plaintext
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot chassis/slot | chassis} lldpdu {tx | rx | tx-and-rx | disable}
```

### Syntax Definitions

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **all**: All LLDP agents.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.
- **chassis**: Specifies the whole chassis.
- **tx**: Transmits LLDPDUs.
- **rx**: Receives LLDPDUs.
- **tx-and-rx**: Transmits and receives LLDPDUs.
- **disable**: Disables LLDPDUs transmission and reception.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>tx</td>
<td>rx</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- The port can be set to receive, transmit, or transmit and receive LLDPDUs using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

**Examples**

```
-> lldp port 1/2 lldpdu tx-and-rx
-> lldp slot 3 lldpdu tx
-> lldp chassis lldpdu disable
```

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

**Related Commands**

- `lldp lldpdu` Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
- `lldp notification` Specifies the switch to control per port notification status about the remote device change.

**MIB Objects**

- `lldpV2PortConfigTable`
  - `lldpV2PortConfigIfIndex`
  - `lldpV2PortConfigDestAddressIndex`
  - `lldpV2PortConfigAdminStatus`
**lldp notification**

Specifies the switch to control per port notification status about the remote device change.

```
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot chassis/slot | chassis} notification {enable | disable}
```

### Syntax Definitions

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **all**: All LLDP agents.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.
- **chassis**: Specifies the whole chassis.
- **enable**: Enables the notification of local system MIB changes.
- **disable**: Disables the notification.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The LLDPDU administrative status must be in the receive state before using this command.
• If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

• Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.

• Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.

• Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples
- `lldp port 1/2 notification enable`
- `lldp slot 1 notification disable`

Release History
Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands
- `lldp notification interval`  Sets the time interval that must elapse before a notification about the local system MIB change is generated.
- `lldp lldpdu`  Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

MIB Objects
- `lldpPortConfigTable`
- `lldpV2PortConfigPortNum`
- `lldpV2PortConfigDestAddressIndex`
- `lldpV2PortConfigNotificationEnable`
lldp network-policy

Configures a local Network Policy on the switch for a specific application type.

```
  lldp network-policy policy_id  application {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} vlan {untagged | priority-tag | vlan_id} [l2-priority 802.1p_value] [dscp dscp_value]
  no lldp network-policy policy_id[-policy_id2]
```

Syntax Definitions

- `policy_id[-policy_id2]` A network policy identifier (0–31) which is associated to a port. Supported only with the `no` form of the command
- `voice` Specifies a voice application type.
- `voice-signaling` Specifies a voice-signaling application type.
- `guest-voice` Specifies a guest-voice application type.
- `guest-voice-signaling` Specifies a guest-voice-signaling application type.
- `softphone-voice` Specifies a softphone-voice application type.
- `video-conferencing` Specifies a video-conferencing application type.
- `streaming-video` Specifies a streaming-video application type.
- `video-signaling` Specifies a video-signaling application type.
- `untagged` Specifies that a VLAN port is untagged.
- `priority-tag` Specifies the internal priority that would be assigned to the VLAN.
- `vlan_id` VLAN identifier. Valid range is 1–4094.
- `802.1p_value` The Layer-2 priority value assigned to the VLAN. Valid range is 0–7.
- `dscp_value` Priority value assigned to the DSCP (Differentiated Service Code Point) header. Valid range is 0–63.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1p_value for voice application</td>
<td>5</td>
</tr>
<tr>
<td>802.1p_value for other applications</td>
<td>0</td>
</tr>
<tr>
<td>dscp_value</td>
<td>0</td>
</tr>
</tbody>
</table>

By default, the VLAN ID is configured in the voice network profile.
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the configured network policy from the system.
- When a network policy is deleted, all the associated values and port bindings are also deleted.
- A maximum of 32 network policies can be configured on a single VLAN.
- Once a policy is created, the application type, VLAN ID, 802.1p, and DSCP values can be modified.
- If a network policy ID is bound to a port, it cannot be modified.
- Use a hyphen to specify a range of Policy IDs and a space to separate multiple Policy IDs in the command.
- The range for Policy IDs is supported only with the no form of this command.

Examples

-> lldp network-policy 10 application voice vlan 20
-> lldp network-policy 11 application guest-voice-signaling vlan untagged l2-priority 3
-> lldp network-policy 20 application voice vlan priority-tag dscp 39
-> lldp network-policy 20 application voice-signaling vlan 23 l2-priority 2 dscp 43
-> no lldp network-policy 10

-> no lldp network-policy 10-20

Release History

Release 8.1.1; command introduced.

Related Commands

lldp tlv med Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
show lldp network-policy Displays the network policy details for a given policy ID.
show lldp med network-policy Displays the network policy configured on a slot or port.
MIB Objects

alaLldpXMedLocMediaPolicyTable
  alaLldpXMedLocMediaPolicyId
  alaLldpXMedLocMediaPolicyAppType
  alaLldpXMedLocMediaPolicyVlanType
  alaLldpXMedLocMediaPolicyVlanID
  alaLldpXMedLocMediaPolicyPriority
  alaLldpXMedLocMediaPolicyDscp
  alaLldpXMedLocMediaPolicyUnknown
  alaLldpXMedLocMediaPolicyTagged
  alaLldpXMedLocMediaPolicyRowStatus
**lldp med network-policy**

 Associates an existing network policy per LLDP agent per port, slot, or chassis. Also specifies the LLDP destination MAC address sent in LLDPDUs.

```
[lldp] [nearest-bridge | nearest-customer | non-tpmr | all] {port chassis/slot/port | slot chassis/slot | chassis} med network-policy policy_id[-policy_id2]

no lldp {port chassis/slot/port | slot chassis/slot | chassis} med network-policy policy_id[-policy_id2]
```

### Syntax Definition

- **nearest-bridge** Specifies the destination MAC address as 01:80:C2:00:00:0E.
- **nearest-customer** Specifies the destination MAC address as 01:80:C2:00:00:00.
- **non-tpmr** Specifies the destination MAC address as 01:80:C2:00:00:03.
- **all** Specifies that all three LLDP agents must be supported.
- **chassis/slot/port[-port2]** The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1-8).
- **chassis/slot** The chassis ID and slot number for a specific module (3/1).
- **chassis** Specifies all switch ports.
- **policy_id[-policy_id2]** A network policy identifier (0–31).

### Defaults

NA

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
<th>9900 X48C4E/V48C8/</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to disassociate a network policy from a port.
- The network policy must already be configured in the system before associating it with a port.
- A maximum of 8 network policies can be associated to a port.
- Two or more network policy IDs with the same application type cannot be associated to a port.

### Examples

```
-> lldp chassis med network-policy 22
-> lldp slot 1/1 med network-policy 1-4 5 6
```
- lldp por 2/1/3 med network-policy 12
- no lldp slot 2/3 med network-policy 12

**Release History**

Release 8.1.1; command introduced.

**Related Commands**

- **lldp tlv med**  
  Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
- **show lldp network-policy**  
  Displays the MED Network Policy details for a given policy ID.
- **show lldp med network-policy**  
  Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

**MIB Objects**

- *alaLldpXMedLocMediaPolicyPortTable*
  - *alaLldpXMedLocMediaPolicyPortIfIndex*
  - *alaLldpXMedLocMediaPolicyId*
  - *alaLldpXMedLocMediaPolicyPortRowStatus*
lldp tlv management

Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

`lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot chassis/slot | chassis} tlv management {port-description | system-name | system-description | system-capabilities | management-address} {enable | disable}`

### Syntax Definitions

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **all**: All LLDP agents.
- **chassis**: The chassis identifier.
- **slot/port1[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.
- **chassis**: Specifies the whole chassis.
- **port-description**: Enables or disables the transmission of port description TLV in LLDPDU.
- **system-name**: Enables or disables the transmission of system name TLV in LLDPDU.
- **system-description**: Enables or disables transmission of system description TLV in LLDPDU.
- **system-capabilities**: Enables or disables transmission of system capabilities TLV in LLDPDU.
- **management-address**: Enables or disables transmission of management address on per port.
- **enable**: Enables management TLV LLDPDU transmission.
- **disable**: Disables management TLV LLDPDU transmission.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable/disable</td>
<td>disable</td>
</tr>
<tr>
<td>non-tpmr</td>
<td>nearest-customer</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

- `lldp port 1/2 tlv management port-description enable`
- `lldp slot 2 tlv management management-address enable`
- `lldp slot 3 tlv management system-name disable`
- `lldp chassis tlv management system-capabilities enable`

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

Related Commands

- **lldp lldpdu**: Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
- **show lldp local-system**: Displays local system information.
- **show lldp local-port**: Displays per port information.
- **show lldp remote-system**: Displays per local port and information of remote system.

MIB Objects

- **lldpV2PortConfigTable**
- **lldpV2LocPortPortNum**
- **lldpV2PortConfigTLVsTxEnable**
lldpV2ConfigManAddrTable
    lldpV2ConfigManAddrPortsTxEnable
**lldp tlv dot1**

Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

```
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot | chassis} tlv dot1 {port-vlan | vlan-name} {enable | disable}
```

**Syntax Definitions**

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **all**: All LLDP agents.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.
- **chassis**: Specifies the whole chassis.
- **port-vlan**: Enables or disables transmission of port VLAN TLV in LLDPDU.
- **vlan-name**: Enables or disables transmission of VLAN name TLV in LLDPDU.
- **enable**: Enables 802.1 TLV LLDPDU transmission.
- **disable**: Disables 802.1 TLV LLDPDU transmission.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>non-tpmr</td>
<td>nearest-customer</td>
</tr>
<tr>
<td>nearest-bridge</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6560</th>
<th>6570M</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- If one TLV is included then the other TLV is automatically included when you use this command.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

**Examples**

-> lldp port 5/1 tlv dot1 port-vlan enable
-> lldp slot 3 tlv dot1 vlan-name enable
-> lldp slot 3 tlv dot1 vlan-name disable

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

**Related Commands**

- **lldp tlv management**
  Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
- **show lldp statistics**
  Displays per port statistics.
- **show lldp local-port**
  Displays per port information.

**MIB Objects**

lldpV2PortConfigTable
  lldpV2PortConfigPortNum
lldpV2Xdot1ConfigPortVlanTable
  lldpV2Xdot1ConfigPortVlanTxEnable
lldpV2Xdot1ConfigVlanNameTable
  lldpV2Xdot1ConfigVlanNameTxEnable
**lldp tlv dot3**

Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

```
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2]| slot chassis/slot | chassis} tlv dot3 [mac-phy][power-via-mdi-measurements] {enable | disable}
```

---

**Syntax Definitions**

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **all**: All LLDP agents.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.
- **chassis**: Specifies the whole chassis.
- **mac-phy**: Allows to transmit MAC and physical configuration status TLV in LLDPDU.
- **power-via-mdi-measurements**: Allows to transmit power via MDI measurements TLV in LLDPDU.
- **enable**: Enables 802.3 TLV LLDPDU transmission.
- **disable**: Disables 802.3 TLV LLDPDU transmission.
### defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>non-tpmr</td>
<td>nearest-customer</td>
</tr>
<tr>
<td>mac-phy</td>
<td>disable</td>
</tr>
<tr>
<td>power-via-mdi-measurements</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

### Examples

- `lldp port 2/4 tlv dot3 mac-phy enable`
- `lldp slot 2 tlv dot3 mac-phy disable`

### Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
Related Commands

**lldp tlv management**
Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

**lldp tlv dot1**
Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

**show lldp statistics**
Displays per port statistics.

MIB Objects

lldpV2PortConfigTable
  lldpV2PortConfigPortNum
lldpV2Xdot3PortConfigTable
  lldpV2Xdot3PortConfigTLVsTxEnable
## lldp tlv med

Specifies the switch to control per port LLDP-MED (Media Endpoint Device) TLVs to be incorporated in the LLDPDUs.

```
lla [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot chassis/slot | chassis} tlv med {power | ext-power-via-mdi | capability} {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>non-tpmr</strong></td>
<td>The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.</td>
</tr>
<tr>
<td><strong>nearest-customer</strong></td>
<td>The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.</td>
</tr>
<tr>
<td><strong>nearest-bridge</strong></td>
<td>The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>All LLDP agents.</td>
</tr>
<tr>
<td><strong>slot</strong></td>
<td>The slot number for a specific module.</td>
</tr>
<tr>
<td><strong>chassis</strong></td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td><strong>power</strong></td>
<td>Enables or disables the power through the MDI TLV in attributes advertised by LLDP.</td>
</tr>
<tr>
<td><strong>ext-power-via-mdi</strong></td>
<td>Enables or disables the extended power through MDI TLV.</td>
</tr>
<tr>
<td><strong>capability</strong></td>
<td>Enables or disables transmission of LLDP-MED capabilities TLV in LLDPDU.</td>
</tr>
<tr>
<td><strong>enable</strong></td>
<td>Enables LLDP-MED TLV LLDPDU transmission.</td>
</tr>
<tr>
<td><strong>disable</strong></td>
<td>Disables LLDP-MED TLV LLDPDU transmission.</td>
</tr>
</tbody>
</table>
802.1AB Commands
lldp tlv med

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>non-tpmr</td>
<td>nearest-customer</td>
</tr>
<tr>
<td>nearest-bridge</td>
<td>nearest-bridge</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command will be lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

```
-> lldp 4/4 tlv med power enable
-> lldp 4/3 tlv med capability enable
-> lldp 4 tlv med power disable
```

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
**Related Commands**

**lldp tlv management**  
Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

**lldp tlv dot1**  
Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

**lldp tlv dot3**  
Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

**MIB Objects**

- `lldpV2PortConfigTable`
  - `lldpV2PortConfigPortNum`
- `lldpV2XMedPortConfigTable`
  - `lldpV2XMedPortConfigTLVStxEnable`
**lldp tlv proprietary**

Allows the switch to advertise the Access Point location through the proprietary TLVs.

```
lldp {port chassis/slot/port|-port2]| slot chassis/slot | chassis} tlv proprietary {enable | disable}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: Slot number for the module and physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
- **slot**: The slot number for a specific module.
- **chassis**: All switch ports.
- **enable**: Enables proprietary TLVs to advertise AP location.
- **disable**: Disables proprietary TLVs to advertise AP location.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The VLAN information is advertised through 802.1x TLV (i.e, Management VLAN is advertised if the port is a 802.1x port else default VLAN of the port is advertised). The AP location is advertised through proprietary TLV.

- If an AP is detected and authenticated on a 802.1x port, LLDP TLVs are triggered to advertise management VLAN and AP location despite CLI configuration being disabled.

- If an AP is removed from 802.1x port, LLDP receives message from 802.1x port after which LLDP stops advertising of management VLAN and AP location, only if the configuration is disabled explicitly on the port.

### Examples

```
-> lldp port 5/1 tlv proprietary enable
-> lldp port 5/1 tlv proprietary disable
-> lldp slot 2 tlv proprietary enable
```
-> lldp slot 2 tlv proprietary disable
-> lldp chassis tlv proprietary enable
-> lldp chassis tlv proprietary disable

**Release History**

Release 8.4.1.R02; command introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp tlv management</td>
<td>Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.</td>
</tr>
<tr>
<td>show lldp statistics</td>
<td>Displays per port statistics.</td>
</tr>
<tr>
<td>show lldp local-port</td>
<td>Displays per port information.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- alaLldpPropConfigTable
- alaLldpPropAPLocation
Illdp tlv application

Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port. This TLV is only configurable for the nearest-bridge LLDP agent.

**Illdp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot chassis/ slot | chassis} tlv application {enable | disable}**

**Syntax Definitions**

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **all**: All LLDP agents.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.
- **chassis**: Specifies the whole chassis.
- **enable**: Enables Application Priority TLV LLDPDU transmission.
- **disable**: Disables Application Priority TLV LLDPDU transmission.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>normal</td>
<td>nearest-customer</td>
</tr>
<tr>
<td>nearest-bridge</td>
<td>nearest-bridge</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The LLDPDU must be enabled and set to transmit before using this command.
• If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

• Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.

• Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.

• Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

-  `lldp port 2/4 tlv application enable`
-  `lldp slot 2 tlv application disable`

Release History

Release 7.3.2; command introduced.

Related Commands

`lldp tlv application priority` Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

`show lldp config` Displays per port statistics.

MIB Objects

-  `lldpXdot1dcbxConfigApplicationPriorityTable`
-  `lldpXdot1dcbxConfigApplicationPriorityTxEnable`
lldp tlv application priority

Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

```
lldp [non-tpmr | nearest-customer | nearest-bridge | all] {port chassis/slot/port[-port2] | slot chassis/slot | chassis} tlv application {fcoe | iscsi | ethtype etype | tcp-sctp-port protocol | udp-dccp-port protocol | port protocol} priority priority
```

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-tpmr</td>
<td>The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.</td>
</tr>
<tr>
<td>nearest-customer</td>
<td>The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.</td>
</tr>
<tr>
<td>nearest-bridge</td>
<td>The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.</td>
</tr>
<tr>
<td>all</td>
<td>All LLDP agents.</td>
</tr>
<tr>
<td>chassis</td>
<td>The chassis identifier when running in virtual chassis mode.</td>
</tr>
<tr>
<td>slot/port[-port2]</td>
<td>The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).</td>
</tr>
<tr>
<td>slot</td>
<td>The slot number for a specific module.</td>
</tr>
<tr>
<td>chassis</td>
<td>Specifies the whole chassis.</td>
</tr>
<tr>
<td>fcoe</td>
<td>Advertise the specified priority value to use for FCoE traffic.</td>
</tr>
<tr>
<td>iscsi</td>
<td>Advertise the specified priority value to use for SCSI traffic.</td>
</tr>
<tr>
<td>etype</td>
<td>Advertise the specified priority value to use for this Ethertype.</td>
</tr>
<tr>
<td>protocol</td>
<td>Advertise the specified priority value to use for the specified protocol.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Usage Guidelines

- The LLDPDU must be enabled and set to transmit and receive before using this command.
- The Application Priority TLV must be enabled for transmission.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.
- Nearest bridge propagation is constrained to a single physical link, packets are stopped by all types of bridges.
- Non-tpmr propagation is constrained by all bridges other than TPMRs, intended for use within provider bridged networks.
- Nearest customer bridge propagation is constrained by customer bridges, this gives the same coverage as a customer-customer MACSec connection.

Examples

- `lldp port 1/1/3 tlv application fcoe priority 3`
- `lldp port 1/1/3 tlv application tcp-sctp-port 3192 priority 5`

Release History

Release 7.3.2; command introduced.

Related Commands

- `lldp tlv application` Enables or disables Application Priority TLV in LLDPDUs.
- `show lldp config` Displays the LLDP port configuration.

MIB Objects

- `alaXdot1dcbxAdminApplicationPriorityAppTable`
- `alaXdot1dcbxAdminApplicationPriorityAEPriority`
**lldp port-id sub-type**

Globally configures the LLDP port to send the interface index or interface name or MAC address in the LLDP Port ID TLV sent in the LLDP packet.

`lldp port-id sub-type {disable | mac-address | name | index}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>mac-address</td>
<td>mac-address</td>
</tr>
<tr>
<td>name</td>
<td>name</td>
</tr>
<tr>
<td>index</td>
<td>index</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>mac-address</td>
<td>mac-address</td>
</tr>
<tr>
<td>name</td>
<td>name</td>
</tr>
<tr>
<td>index</td>
<td>index</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The configuration is applied to all the ports in the switch irrespective of the device connected at the other end of the switch.
- The configuration can be applied to a specific chassis, slot and port using the `lldp port med-device` CLI.
- The global configuration will over ride the port level configuration.

**Examples**

- `-> lldp port-id sub-type mac-address`
- `-> lldp port-id sub-type name`
- `-> lldp port-id sub-type index`
- `-> lldp port-id sub-type disable`
Release History
Release 8.8R2; command introduced.

Related Commands

- **lldp port med-device**: Configures a specific chassis, slot and port to send the interface index or interface name or MAC address in the LLDP Port ID TLV sent in the LLDP packet.

- **show lldp config**: Displays the general LLDP configuration information for LLDP ports.

MIB Objects

- **alaLldpV2PropConfigTable**
- **alaLLDPConfigPortIdSubType**
**lldp port med-device**

Configures a specific chassis, slot and port to send the interface index or interface name or MAC address in the LLDP Port ID TLV sent in the LLDP packet.

    lldp port chassis/slot/port med-device port-id sub-type {mac-address | name | index}

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>Includes the MAC address in the LLDP port ID TLV sent in the LLDP packet.</td>
</tr>
<tr>
<td>name</td>
<td>Includes the interface name in the LLDP port ID TLV sent in the LLDP packet.</td>
</tr>
<tr>
<td>index</td>
<td>Includes the interface index in the LLDP port ID TLV sent in the LLDP packet.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>mac-address</td>
</tr>
<tr>
<td>name</td>
<td></td>
</tr>
<tr>
<td>index</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The configuration is applied to a specific chassis, slot and port in the switch.
- The global configuration will over ride the port level configuration.
- To enable the port level configuration the global configuration must be disabled using the lldp port-id sub-type CLI.

**Examples**

- `lldp port 1/1/1 med-device port-id sub-type mac-address`
- `lldp port 1/1/1 med-device port-id sub-type name`
- `lldp port 1/1/1 med-device port-id sub-type index`
- `lldp port-id sub-type disable`

**Release History**

Release 8.8R2; command introduced.
**Related Commands**

- **lldp port-id sub-type**
  Globally configures the LLDP port to send the interface index or interface name or MAC address in the LLDP Port ID TLV sent in the LLDP packet.

- **show lldp config**
  Displays the general LLDP configuration information for LLDP ports.

**MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaLldpV2PropConfigTable</td>
</tr>
<tr>
<td>alaLldpV2PropPortIdSubType</td>
</tr>
</tbody>
</table>
lldp chassis-mac-delimiter

Configures the MAC address delimiter to be sent with the MAC address when the client server queries the switch for chassis MAC address.

```
lldp chassis-mac-delimiter {colon | dash | none}
```

### Syntax Definitions

- **colon** Sends the MAC address with colon to the client server.
- **dash** Sends the MAC address with dash to the client server.
- **none** Sends the MAC address without delimiter to the client server.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>colon</td>
<td>dash</td>
</tr>
<tr>
<td>colon</td>
<td>colon</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

| 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 | 6900 |
|  |  |  |  |  |  |  |  | C32E/T24C2/ | X24C2 |
| No | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

### Usage Guidelines

N/A

### Examples

```
-> lldp chassis-mac-delimiter colon
-> lldp chassis-mac-delimiter dash
-> lldp chassis-mac-delimiter none
```

### Release History

Release 8.8R2; command introduced.
Related Commands

**show lldp local-system** Displays local system information.

MIB Objects

alaLldpV2PropConfigTable
  alaLLDPConfigChasMACDelim
show lldp system-statistics

Displays system-wide statistics.

show lldp system-statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show lldp system-statistics
Local LLDP Agent System Statistics:
  Remote Systems Last Change = 0 days 0 hours 3 minutes and 10 seconds,
  Remote Systems MIB Inserts = 2,
  Remote Systems MIB Deletes = 0,
  Remote Systems MIB Drops = 0,
  Remote Systems MIB Age Outs = 0

output definitions

<table>
<thead>
<tr>
<th>Output Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Systems Last Change</td>
<td>The last change recorded in the tables associated with the remote system.</td>
</tr>
<tr>
<td>Remote Systems MIB Inserts</td>
<td>The total number of complete inserts in the tables associated with the remote system.</td>
</tr>
<tr>
<td>Remote Systems MIB Deletes</td>
<td>The total number of complete deletes in tables associated with the remote system.</td>
</tr>
<tr>
<td>Remote Systems MIB Drops</td>
<td>The total number of LLDPDUs dropped because of insufficient resources.</td>
</tr>
<tr>
<td>Remote Systems MIB Age Outs</td>
<td>The total number of complete age-outs in the tables associated with the remote system.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **lldp notification**
  Specifies the switch to control per port notification status about the remote device change.

- **lldp notification interval**
  Sets the time interval that must elapse before a notification about the local system MIB change is generated.

**MIB Objects**

- **lldpStatistics**
  - **lldpStatsRemTablesLastChangeTime**
  - **lldpStatsRemTablesInserts**
  - **lldpStatsRemTablesDeletes**
  - **lldpStatsRemTablesDrops**
  - **lldpStatsRemTablesAgeouts**
show lldp statistics

Displays per port statistics.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port[-port2] slot chassis/slot] statistics

Syntax Definitions

non-tpmr The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.

nearest-customer The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.

nearest-bridge The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.

chassis The chassis identifier.

slot/port[-port2] The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

slot The slot number for a specific module.

Defaults

By default, statistics for all LLDP ports are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the slot/port option is not specified, statistics for the chassis are displayed.
- If the statistics are zero they are not displayed.

Examples

`-> show lldp statistics

Slot/Port  LLDPDU  LLDPDU  LLDPDU  LLDPDU  TLV  TLV  Device
          Tx      TxLenErr Rx Errors Discards Unknown Discards Ageouts
---------+---------+---------+---------+---------+---------+---------+---------+--------+--------+---------+---------+--------+--------+--------+--------+--------+
 1/1      453     0       452     0       0       0       0       0       0       0
 1/2      452     0       453     0       0       0       0       0       0       0
 1/5      452     0       473     0       0       476     476     0       0       0
 1/8      455     0       464     0       0       0       0       0       0       0
 1/9      456     0       464     0       0       0       0       0       0       0

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 17-46
802.1AB Commands

```
1/10  454  0  464  0  0  0  0  0
1/11  453  0  447  0  0  0  0  0
1/12  453  0  0  0  0  0  0  0
1/13  453  0  0  0  0  0  0  0
1/14  453  0  0  0  0  0  0  0
1/17  453  0  963  0  0 449  449  0
1/18  453  0  0  0  0  0  0  0
2/1  452  0  457  0  0  0  0  0
2/2  452  0  963  0  0  0  0  0
2/3  480  0  459  0  0  0  0  2
```

**output definitions**

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot/Port</td>
<td>Slot number for the module and physical port number on that module.</td>
</tr>
<tr>
<td>LLDPDU Tx</td>
<td>The total number of LLDPDUs transmitted on the port.</td>
</tr>
<tr>
<td>LLDPDU Rx</td>
<td>The total number of valid LLDPDUs received on the port.</td>
</tr>
<tr>
<td>LLDPDU Errors</td>
<td>The total number of invalid LLDPDUs discarded on the port.</td>
</tr>
<tr>
<td>LLDPDU Discards</td>
<td>The total number of LLDPDUs discarded on the port.</td>
</tr>
<tr>
<td>TLV Unknown</td>
<td>The total number of unrecognized LLDP TLVs on the port.</td>
</tr>
<tr>
<td>TLV Discards</td>
<td>The total number of LLDP TLVs discarded on the port.</td>
</tr>
<tr>
<td>Device Ageouts</td>
<td>The total number of complete age-outs on the port.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

**Related Commands**

- `lldp lldpdu` Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.
- `lldp tlv management` Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

**MIB Objects**

```
lldpV2StatsTxPortTable
    lldpV2StatsTxPortNum
    lldpV2StatsTxPortFramesTotal

lldpV2StatsRxPortTable
    lldpV2StatsRxPortNum
    lldpV2StatsRxPortFramesDiscardedTotal
    lldpV2StatsRxPortFramesErrors
    lldpV2StatsRxPortFramesTotal
    lldpV2StatsRxPortTLVsDiscardedTotal
    lldpV2StatsRxPortTLVsUnrecognizedTotal
    lldpV2StatsRxPortAgeoutsTotal
```
show lldp local-system

Displays local system information.

show lldp local-system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show lldp local-system
Local LLDP Agent System Data:
  Chassis ID Subtype       = 4 (MAC Address),
  Chassis ID               = 00:d0:95:e9:c9:2e,
  System Name              = OS6900-DC1,
  System Description       = 7.3.2.315.R01 Development, June 03, 2013.,
  Capabilities Supported   = Bridge, Router,
  Capabilities Enabled     = Bridge, Router,
  LLDPDU Transmit Interval = 30 seconds,
  TTL Hold Multiplier      = 4,
  LLDPDU Transmit Delay    = 2 seconds,
  Reinitialization Delay   = 2 seconds,
  MIB Notification Interval= 5 seconds
  Management Address Type  = 1 (IPv4),
  Management IP Address    = 10.255.11.100,
  LLDP Port ID SubType     = Disable,
  Chassis MAC Delimiter    = colon,

output definitions

<table>
<thead>
<tr>
<th>Chassis ID Subtype</th>
<th>The subtype that describe chassis ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID</td>
<td>The chassis ID (MAC address).</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>The name of the system.</td>
</tr>
<tr>
<td>System Description</td>
<td>The description of the system.</td>
</tr>
<tr>
<td>Capabilities Supported</td>
<td>The capabilities of the system.</td>
</tr>
<tr>
<td>Capabilities Enabled</td>
<td>The enabled capabilities of the system.</td>
</tr>
<tr>
<td>LLDPDU Transmit Interval</td>
<td>The LLDPDU transmit interval.</td>
</tr>
<tr>
<td>TTL Hold Multiplier</td>
<td>The hold multiplier used to calculate TTL.</td>
</tr>
<tr>
<td>LLDPDU Transmit Delay</td>
<td>The minimum transmit time between successive LLDPDUs.</td>
</tr>
<tr>
<td>Reinitialization Delay</td>
<td>The minimum time interval before the reinitialization of local port objects between port status changes.</td>
</tr>
<tr>
<td>MIB Notification Interval</td>
<td>The minimum time interval between consecutive notifications of local system MIB change.</td>
</tr>
<tr>
<td>Management Address Type</td>
<td>The type of management address used in LLDPDU.</td>
</tr>
<tr>
<td>Management IP Address</td>
<td>The management IP address. The loopback0 IP address is configured for the management IP address to be transmitted.</td>
</tr>
<tr>
<td>LLDP Port ID SubType</td>
<td>Displays if the LLDP Port ID subtype is configured.</td>
</tr>
<tr>
<td>Chassis MAC Delimiter</td>
<td>Displays the configured chassis MAC delimiter.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
Release 8.8R2; **LLDP Port ID SubType** and **Chassis MAC Delimiter** output fields added.

**Related Commands**

- `lldp reinit delay`: Sets the time interval that must elapse before the current status of a port is reinitialized after a status change.
- `lldp transmit hold-multiplier`: Sets the transmit hold multiplier value, which is used to calculate the Time To Live TLV.
- `lldp transmit interval`: Sets the minimum time interval between successive LLDPDUs transmitted.
- `lldp chassis-mac-delimiter`: Configures the MAC address delimiter to be sent with the MAC address when the client server queries the switch for chassis MAC address.

**MIB Objects**

- `lldpV2LocalSystemData`:
  - `lldpV2LocChassisIdSubtype`
  - `lldpV2LocChassisId`
  - `lldpV2LocSysName`
  - `lldpV2LocSysDesc`
  - `lldpV2LocSysCapSupported`
  - `lldpV2LocSysEnabled`
- `lldpV2PortConfigTable`:
  - `lldpV2MessageTxInterval`
  - `lldpV2MessageTXHoldMultiplier`
802.1AB Commands

show lldp local-system

lldpV2TxDelay
lldpV2ReinitDelay
lldpV2NotificationInterval
lldpV2LocManAddrTable
  lldpV2LocManAddrSubtype
  lldpV2LocManAddr
alaLldpV2PropConfigTable
  alaLLDPConfigPortIdSubType
  alaLldpV2PropPortIdSubType
  alaLLDPConfigChasMACDelim
**show lldp local-port**

Displays per-port information.

```plaintext
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port[-port2]] slot chassis/slot] local-port
```

### Syntax Definitions

- **non-tpmr**  
  The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.

- **nearest-customer**  
  The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.

- **nearest-bridge**  
  The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.

- **chassis**  
  The chassis identifier.

- **slot/port[-port2]**  
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **slot**  
  The slot number for a specific module.

### Defaults

By default, a list of all LLDP ports is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show lldp local-port
Local Port 1/1/1 LLDP Info:
  Port ID = 1001 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 XNI 1/1/1,
  Vlan = 1,
  AP Location = sw1,
Local Port 1/1/2 LLDP Info:
  Port ID = 1002 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 XNI 1/1/2,
  Vlan = 1,
```

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 17-51
AP Location = -, Local Port 1/1/3 LLDP Info:
  Port ID = 1003 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/3,
  Vlan = 1,
  AP Location = -,
Local Port 1/1/4 LLDP Info:
  Port ID = 1004 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/4,
  Vlan = 1,
  AP Location = -,
Local Port 1/1/5 LLDP Info:
  Port ID = 1005 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/5,
  Vlan = 1,
  AP Location = -,
Local Port 1/1/6 LLDP Info:
  Port ID = 1006 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/6,
  Vlan = 4095,
  AP Location = -,
Local Port 1/1/7 LLDP Info:
  Port ID = 1007 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/7,
  Vlan = 1,
  AP Location = -,
Local Port 1/1/8 LLDP Info:
  Port ID = 1008 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/8,
  Vlan = 1,
  AP Location = -,
Local Port 1/1/9 LLDP Info:
  Port ID = 1009 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/9,
  Vlan = 4095,
  AP Location = -,
Local Port 1/1/10 LLDP Info:
  Port ID = 1010 (Locally assigned),
  Port Description = Alcatel-Lucent OS6865 GNI 1/1/10,
  Vlan = 4095,
  AP Location = -,

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port ID</td>
<td>The port ID (port MAC).</td>
</tr>
<tr>
<td>Port Description</td>
<td>The description of the port (which includes the port number and the AOS version).</td>
</tr>
<tr>
<td>Vlan</td>
<td>Displays the authenticated VLAN (management VLAN) if AP is connected on a dot1x enabled port, else the default VLAN of the port is displayed.</td>
</tr>
<tr>
<td>AP Location</td>
<td>Displays the location to which the AP is connected.</td>
</tr>
</tbody>
</table>
Release History
Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
Release 8.4.1.R02; Vlan and AP Location output fields added.

Related Commands

**lldp tlv management** Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

**lldp tlv dot1** Specifies the switch to control per port 802.1 TLVs to be incorporated in the LLDPDUs.

**lldp tlv proprietary** Allows the switch to advertise the Access Point location through the proprietary TLVs.

MIB Objects

`lldpV2LocPortTable`
- `lldpV2LocPortNum`
- `lldpV2LocPortId subtype`
- `lldpV2LocPortId`
- `lldpV2LocPortDesc`
- `alaLldpPropAPLocation`
- `alaLldpPropVlan`
- `alaLldpPropLocationDesc`
show lldp local-management-address

Displays the local management address information.

show lldp local-management-address

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show lldp local-management-address
Local LLDP Agent Management Address:
  Management Address Type = 1 (IPv4),
  Management IP Address = 10.255.11.100

output definitions

<table>
<thead>
<tr>
<th>Management Address Type</th>
<th>The address type used to define the interface number (IPv4 or IPv6).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP Address</td>
<td>The management IP address. The loopback0 IP address is configured for the management IP address to be transmitted.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.
**Related Commands**

- `lldp tlv management` Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
- `show lldp local-system` Displays local system information.

**MIB Objects**

- `lldpV2LocManAddrTable`
- `lldpV2LocManAddrLen`
- `lldpV2LocManAddrIfSubtype`
- `lldpV2LocManAddrIfId`
show lldp config

Displays the general LLDP configuration information for LLDP ports.

```
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis[/slot[/port[/[-port2]]]] [slot chassis/slot] config [application-tlv]
```

### Syntax Definitions

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.
- **application-tlv**: Displays Application Priority TLV parameters.

### Defaults

By default, a list of all LLDP ports with their configuration parameters is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `slot/port` or `slot` parameter to display information for a specific port or for all ports on a specific module.

### Examples

```
-> show lldp config
Chas/ Slot/Port Status  Admin  Notify  Std TLV  Mgmt  802.1  802.3 MED  App-Prio  Trust  Proprietary  Port-Id
      Admin  Notify  Std TLV  Mgmt  802.1  802.3 MED  App-Prio  Trust  Proprietary  Port-Id
---------+-------+--------+-------+--------+--------+-----+----+--------+--------+-----------+---------
1/1/1     Rx + Tx Disabled 0x10 Disabled Disabled 0x00 0x00 Disabled Disabled Disabled      Mac
1/1/2     Rx + Tx Disabled 0x10 Disabled Disabled 0x00 0x00 Disabled Disabled Disabled      Mac
1/1/3     Rx + Tx Disabled 0x10 Disabled Disabled 0x00 0x00 Disabled Disabled Disabled      Mac
1/1/4     Rx + Tx Disabled 0x10 Disabled Disabled 0x00 0x00 Disabled Disabled Disabled      Mac
1/1/5     Rx + Tx Disabled 0x10 Disabled Disabled 0x00 0x00 Disabled Disabled Disabled      Mac
1/1/6     Rx + Tx Disabled 0x10 Disabled Disabled 0x00 0x00 Disabled Disabled Disabled      Mac

```
### 802.1AB Commands

```
1/1/7  Rx + Tx Disabled  0x10   Disabled  Disabled 0x00 0x00 Disabled Disabled Disabled  Mac
1/1/8  Rx + Tx Disabled  0x10   Disabled  Disabled 0x00 0x00 Disabled Disabled Disabled  Mac
1/1/9  Rx + Tx Disabled  0x10   Disabled  Disabled 0x00 0x00 Disabled Disabled Disabled  Mac
1/1/10 Rx + Tx Disabled  0x10   Disabled  Disabled 0x00 0x00 Disabled Disabled Disabled  Mac

-> show lldp config application-tlv
Chas/Slot/Port Selector Protocol Priority
------------------------------+-----------+------------+
1/1/2  Ethertype          0x8906        3
1/1/2  Tcp/Sctp            3260          4
1/1/20 Tcp/Sctp            3190          3
1/1/20 Udp/Dccp           300           4
1/1/20 Tcp/Udp/Sctp/Dccp   300           4
```

**output definitions**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chas/Slot/Port</td>
<td>The LLDP slot and port number.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Indicates the Administrative status of the LLDP port. The options are: Disabled, Rx, Tx, and Rx+Tx.</td>
</tr>
<tr>
<td>Notify Trap</td>
<td>Indicates whether the Notify Trap feature is disabled or enabled on a particular port.</td>
</tr>
<tr>
<td>Std TLV Mask</td>
<td>The standard TLV mask set for the port.</td>
</tr>
<tr>
<td>Mgmt Address</td>
<td>Indicates whether transmission of the per port IPv4 management address is enabled or disabled.</td>
</tr>
<tr>
<td>802.1 TLV</td>
<td>Indicates whether 802.1 TLV status is enabled or disabled on the LLDP port.</td>
</tr>
<tr>
<td>802.3 Mask</td>
<td>The standard 802.3 mask set for the port.</td>
</tr>
<tr>
<td>MED Mask</td>
<td>The standard MED mask set for the port.</td>
</tr>
<tr>
<td>App-Prio TLV</td>
<td>Indicates the Application priority TLV status.</td>
</tr>
<tr>
<td>Trust Status</td>
<td>Indicates the Trust Status.</td>
</tr>
<tr>
<td>Proprietary TLV</td>
<td>Indicates the proprietary TLV status.</td>
</tr>
<tr>
<td>Port-Id TLV</td>
<td>Displays what is included in the LLDP Port ID TLV sent in the LLDP packet.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 7.3.2; **App-Prio TLV** field added, **application-tlv** parameter added.
Release 7.3.1; Version 2 (2009) updates implemented.
Release 8.4.1.R02; **Proprietary TLV** output field added.
Release 8.8R2; **Port-Id TLV** output field added.
**Related Commands**

**lldp lldpdu**
Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, a slot, or a port.

**lldp notification**
Specifies the switch to control per port notification status about the remote device change.

**lldp tlv management**
Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.

**lldp tlv dot3**
Specifies the switch to control per port 802.3 TLVs to be incorporated in the LLDPDUs.

**lldp tlv application**
Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port.

**lldp tlv application priority**
Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

**lldp port-id sub-type**
Globally configures the LLDP port to send the interface index or interface name or MAC address in the LLDP Port ID TLV sent in the LLDP packet.

**lldp port med-device**
Configures a specific chassis, slot and port to send the interface index or interface name or MAC address in the LLDP Port ID TLV sent in the LLDP packet.

**MIB Objects**

**lldpV2PortConfigTable**
- **lldpV2PortConfigPortNum**
- **lldpV2PortConfigAdminStatus**
- **lldpV2PortConfigNotificationEnable**
- **lldpV2LocPortPortNum**
- **lldpV2PortConfigTLVsTxEnable**

**lldpV2ConfigManAddrTable**
- **lldpV2ConfigManAddrPortTxEnable**

**lldpV2Xdot3PortConfigTable**
- **lldpV2Xdot3PortConfigTLVsTxEnable**

**lldpV2Xdot1dcbxConfigApplicationPriorityTable**
- **lldpV2Xdot1dcbxConfigApplicationPriorityTxEnable**

**alaXdot1dcbxAdminApplicationPriorityAppTable**
- **alaXdot1dcbxAdminApplicationPriorityAPriority**
show lldp network-policy

Displays the MED Network Policy details for a given policy ID.

show lldp network-policy [policy_id]

Syntax Definitions

policy_id

Policy identifier for a network policy definition. Valid range is between 0 and 31.

Defaults

By default, all configured policies are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Network policy must be configured on the system before using this command.
- Enter a policy ID with this command to display information for a specific policy.

Examples

-> show lldp network-policy
Legend: 0 Priority Tagged Vlan
   - Untagged Vlan

<table>
<thead>
<tr>
<th>Network Policy ID</th>
<th>Application Type</th>
<th>Vlan</th>
<th>Layer2</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Id</td>
<td>Priority</td>
<td>Value</td>
</tr>
<tr>
<td>1</td>
<td>voice</td>
<td>4000</td>
<td>7</td>
<td>33</td>
</tr>
<tr>
<td>12</td>
<td>guest-voice</td>
<td>-</td>
<td>-</td>
<td>44</td>
</tr>
<tr>
<td>21</td>
<td>streaming-voice</td>
<td>0</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td>31</td>
<td>guest-voice-signaling</td>
<td>23</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

-> show lldp network-policy 21
Legend: 0 Priority Tagged Vlan
   - Untagged Vlan

<table>
<thead>
<tr>
<th>Network Policy ID</th>
<th>Application Type</th>
<th>Vlan</th>
<th>Layer2</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Id</td>
<td>Priority</td>
<td>Value</td>
</tr>
<tr>
<td>21</td>
<td>streaming-voice</td>
<td>0</td>
<td>4</td>
<td>11</td>
</tr>
</tbody>
</table>
## show lldp network-policy

### Command Description

Configures a local network policy on a switch for an application type.

### Output Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Policy ID</strong></td>
<td>Policy identifier for a network policy definition.</td>
</tr>
<tr>
<td><strong>Application Type</strong></td>
<td>Indicates the type of application configured on the port or VLAN.</td>
</tr>
<tr>
<td><strong>VLAN ID</strong></td>
<td>The VLAN ID assigned to the port on which the network policy is configured.</td>
</tr>
<tr>
<td><strong>Layer2 Priority</strong></td>
<td>Layer 2 priority to be used for the specified application type.</td>
</tr>
<tr>
<td><strong>DSCP Value</strong></td>
<td>DSCP value to be used to provide Diffserv node behavior for the specified application type.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.1.1 command introduced.

### Related Commands

- **lldp network-policy**: Configures a local network policy on a switch for an application type.

### MIB Objects

- alaLldpXMedLocMediaPolicyTable
  - alaLldpXMedLocMediaPolicyId
  - alaLldpXMedLocMediaPolicyAppType
  - alaLldpXMedLocMediaPolicyVlanType
  - alaLldpXMedLocMediaPolicyVlanId
  - alaLldpXMedLocMediaPolicyPriority
  - alaLldpXMedLocMediaPolicyDscp
  - alaLldpXMedLocMediaPolicyUnknown
  - alaLldpXMedLocMediaPolicyTagged
show lldp med network-policy

Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

show lldp [nearest-bridge | nearest-customer | non-tpmr | all] [slot chassis/slot | port chassis/slot/port] med network-policy

**Syntax Definitions**

**nearest-bridge** The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.

**nearest-customer** The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.

**non-tpmr** The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.

**all** Specifies that all three LLDP agents must be supported.

**chassis/slot** The chassis ID and slot number for a specific module (3/1).

**chassis/slot/port[-port2]** The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).

**Defaults**

By default, all ports with associated policies are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Network policy must be configured on the system before using this command.
- Enter a slot or slot/port number with this command to display information for a specific slot or port.

**Examples**

```bash
-> show lldp slot 1/1 med network-policy
Chas/
Slot/Port      Network Policy ID
-------------------------------------
1/1/1           1 3 5 7 21 23 30 31
1/1/2           1 2 3 4 7 8 9 10
```
**output definitions**

<table>
<thead>
<tr>
<th>Chassis/Slot/Port</th>
<th>Slot number for the module and physical port number on that module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy ID</td>
<td>Policy identifier for a network policy definition.</td>
</tr>
</tbody>
</table>

**Release History**
Release 8.1.1; command introduced.

**Related Commands**
- `lldp tlv med` Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
- `lldp med network-policy` Configures a local network policy on a switch for an application type.

**MIB Objects**

<table>
<thead>
<tr>
<th>alaLldpXMedLocMediaPolicyPortTable</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaLldpXMedLocMediaPolicyPortIfIndex</td>
</tr>
<tr>
<td>alaLldpXMedLocMediaPolicyId</td>
</tr>
</tbody>
</table>
show lldp remote-system

Displays per local port and information of remote system.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port[-port2] | slot chassis/slot] remote-system

---

### Syntax Definitions

- **non-tpmr**: The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.
- **nearest-customer**: The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.
- **nearest-bridge**: The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **slot**: The slot number for a specific module.

### Defaults

By default, a list of all lldp ports is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show lldp remote-system
Remote LLDP Agents on Local Slot/Port: 2/47,
  Chassis ID Subtype  = 4 (MAC Address),
  Chassis ID         = 00:d0:95:e9:c9:2e,
  Port ID Subtype    = 7 (Locally assigned),
  Port ID            = 2048,
  Port Description   = (null),
  System Name        = (null),
  System Description = (null),
  Capabilities Supported = none supported,
```
Capabilities Enabled = none enabled,

Remote LLDP Agents on Local Slot/Port: 2/48,
  Chassis ID Subtype = 4 (MAC Address),
  Chassis ID = 00:d0:95:e9:c9:2e,
  Port ID Subtype = 7 (Locally assigned),
  Port ID = 2047,
  Port Description = (null),
  System Name = (null),
  System Description = (null),
  Capabilities Supported = none supported,
  Capabilities Enabled = none enabled,

**output definitions**

<table>
<thead>
<tr>
<th>Remote LLDP Agents on Local Slot/Port</th>
<th>The Slot number to which the remote system entry is associated and the physical port number on that module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID Subtype</td>
<td>The sub type that describes chassis ID.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The chassis ID (MAC address).</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The sub type that describes port ID</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port ID (Port MAC).</td>
</tr>
<tr>
<td>Port Description</td>
<td>The description of the port (which includes the port number and the AOS version).</td>
</tr>
<tr>
<td>System Name</td>
<td>The name of the system.</td>
</tr>
<tr>
<td>System Description</td>
<td>The description of the system.</td>
</tr>
<tr>
<td>Capabilities Supported</td>
<td>The capabilities of the system.</td>
</tr>
<tr>
<td>Capabilities Enabled</td>
<td>The enabled capabilities of the system.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

**Related Commands**

- `show lldp local-port` Displays per port information.
- `show lldp local-system` Displays local system information.

**MIB Objects**

- `lldpV2RemTable`
  - `lldpV2RemLocalPortNum`
  - `lldpV2RemChassisIdSubtype`
  - `lldpV2RemChassisId`
  - `lldpV2RemPortIdSubtype`
  - `lldpV2RemPortId`
  - `lldpV2RemPortDesc`
  - `lldpV2RemSysName`
  - `lldpV2RemSysDesc`
  - `lldpV2RemSysCapSupported`
  - `lldpV2RemSysCapEnabled`
  - `lldpV2RemManAddrIfSubtype`
lldpV2RemManAddrIfId
show lldp remote-system med

Displays remote system MED information for a single port or all ports on a slot.

show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port[-port2] | slot chassis/slot] remote-system med {network-policy | inventory}

Syntax Definitions

**non-tpmr**
The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.

**nearest-customer**
The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.

**nearest-bridge**
The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.

**chassis**
The chassis identifier.

**slot/port[-port2]**
The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

**slot**
The slot number for a specific module.

**network-policy**
Display network-policy TLVs from remote Endpoint Devices.

**inventory**
Display inventory management TLVs from remote Endpoint Devices.

Defaults

By default, a list of all LLDP ports is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `slot/port` or `slot` parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp port 2/47 remote-system med network-policy
Slot/ Remote Application Unknown Tagged Vlan Layer2 DSCP
Port   ID   Type  Policy Flag Tag Flag Id   Priority Value
------- ------- -------- ---------- -------- -------- ------ -------- ----
1/22   1     Voice(01) Defined Untagged 345     4       34
1/22   2     Guest Voice(4) Defined Untagged 50      3       46
```
output definitions

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>The Slot number to which the remote system entry is associated and the physical port number on that module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote ID</td>
<td>The Index of the Remote Device.</td>
</tr>
<tr>
<td>Application Type</td>
<td>The Application type of the peer entity.</td>
</tr>
<tr>
<td>1. Voice</td>
<td></td>
</tr>
<tr>
<td>2. Voice Signaling</td>
<td></td>
</tr>
<tr>
<td>3. Guest Voice</td>
<td></td>
</tr>
<tr>
<td>4. Guest Voice Signaling</td>
<td></td>
</tr>
<tr>
<td>5. Softphone Voice</td>
<td></td>
</tr>
<tr>
<td>6. Video Conferencing</td>
<td></td>
</tr>
<tr>
<td>7. Streaming Video</td>
<td></td>
</tr>
<tr>
<td>8. Video Signaling</td>
<td></td>
</tr>
<tr>
<td>Unknown Policy Flag</td>
<td>Whether the network policy for the specified application type is currently defined or unknown.</td>
</tr>
<tr>
<td>Tagged Flag</td>
<td>Whether the specified application type is using a tagged or an untagged VLAN.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN identifier (VID) for the port.</td>
</tr>
<tr>
<td>Layer 2 Priority</td>
<td>Layer 2 priority to be used for the specified application type.</td>
</tr>
<tr>
<td>DSCP Value</td>
<td>DSCP value to be used to provide Diffserv node behavior for the specified application type.</td>
</tr>
</tbody>
</table>

-> show lldp port 2/47 remote-system med inventory
Remote LLDP Agents on Local Slot/Port 1/22:
  Remote ID  1:
    MED Hardware Revision = "1.2.12.3",
    MED Firmware Revision = "7.3.2.1",
    MED Software Revision = "4.2.1.11",
    MED Serial Number = "32421",
    MED Manufacturer Name = "Manufacturer1",
    MED Model Name = "Alc32d21",
    MED Asset ID = "124421",
  Remote ID  2:
    MED Hardware Revision = "1.2.12.4",
    MED Firmware Revision = "7.3.2.2",
    MED Software Revision = "4.2.1.13",
    MED Serial Number = "32424",
    MED Manufacturer Name = "Manufacturer2",
    MED Model Name = "Alc32d41",
    MED Asset ID = "124424",

output definitions

<table>
<thead>
<tr>
<th>Remote ID</th>
<th>The Index of the Remote Device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MED Hardware Revision</td>
<td>The Hardware Revision of the endpoint</td>
</tr>
<tr>
<td>MED Firmware Revision</td>
<td>The Firmware Revision of the endpoint.</td>
</tr>
<tr>
<td>MED Software Revision</td>
<td>The Software Revision of the endpoint.</td>
</tr>
<tr>
<td>MED Manufacturer Name</td>
<td>The Manufacturer Name of the endpoint.</td>
</tr>
<tr>
<td>MED Model Name</td>
<td>The Model Name of the endpoint.</td>
</tr>
<tr>
<td>MED Asset ID</td>
<td>The Asset ID of the endpoint.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; Version 2 (2009) updates implemented.

**Related Commands**

- `show lldp local-port` Displays per port information.
- `show lldp local-system` Displays local system information.

**MIB Objects**

- `lldpV2XMedRemMediaPolicyTable`
  - `lldpV2XMedRemMediaPolicyAppType`
  - `lldpV2XMedRemMediaPolicyDscp`
  - `lldpV2XMedRemMediaPolicyPriority`
  - `lldpV2XMedRemMediaPolicyTagged`
  - `lldpV2XMedRemMediaPolicyUnknown`
  - `lldpV2XMedRemMediaPolicyVlanID`
- `lldpV2XMedRemInventoryTable`
  - `lldpV2XMedRemAssetID`
  - `lldpV2XMedRemFirmwareRev`
  - `lldpV2XMedRemHardwareRev`
  - `lldpV2XMedRemMfgName`
  - `lldpV2XMedRemModelName`
  - `lldpV2XMedRemSerialNum`
  - `lldpV2XMedRemSoftwareRev`
**show lldp remote-system application-tlv**

Displays remote system Application Priority TLV information for a single port or all ports on a slot.

```
show lldp [non-tpmr | nearest-customer | nearest-bridge] [port chassis/slot/port|-port2] | slot chassis/slot] remote-system application-tlv
```

### Syntax Definitions

**non-tpmr**  
The non-TPMR agent using destination MAC address 01-80-C2-00-00-03.

**nearest-customer**  
The nearest customer bridge agent using destination MAC address 01-80-C2-00-00-00.

**nearest-bridge**  
The nearest bridge agent using destination MAC address 01-80-C2-00-00-0E.

**chassis**  
The chassis identifier.

**slot/port[-port2]**  
The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

**slot**  
The slot number for a specific module.

### Defaults

By default, a list of all LLDP ports is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `slot/port` or `slot` parameter to display information for a specific port or for all ports on a specific module.

### Examples

```
-> show lldp remote-system application-tlv
Slot/ Port     Remote ID Selector  Protocol  Priority
-------------+-------+----------+-----------+------------+--------+----------+-----------+----------+----------------+
1/2          1     Ethertype  35078      3 [fcce]  
1/2          1     Tcp/Sctp  3260       4 [iscsi]  
1/20         1     Tcp/Sctp  3190       3        
1/20         1     Udp/Dccp  300        4        
1/20         1     Tcp/Udp/Sctp/Dccp 300      4        
```
output definitions

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>The Slot number to which the remote system entry is associated and the physical port number on that module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote ID</td>
<td>The Index of the Remote Device.</td>
</tr>
<tr>
<td>Selector</td>
<td>The protocol selector.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol Ethertype or well-known port.</td>
</tr>
<tr>
<td>Priority</td>
<td>The 802.1p priority value for the specified protocol to use.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command introduced.

Related Commands

lldp tlv application    Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port.

lldp tlv application priority Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

show lldp config       Displays the general LLDP configuration information for LLDP ports.

MIB Objects

alaXdot1dcbxAdminApplicationPriorityAppTable
alaXdot1dcbxAdminApplicationPriorityAESelector
alaXdot1dcbxAdminApplicationPriorityAEPriority
alaXdot1dcbxAdminApplicationPriorityAEPriority
### show lldp remote-system power-via-mdi

Displays the information of remote system which includes the information received in the power via MDI TLV.

```plaintext
show lldp [port chassis/slot/port[-port2] | slot chassis/slot] remote-system power-via-mdi
```

#### Syntax Definitions

- `chassis`  
  The chassis identifier.
- `slot/port[-port2]`  
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `slot`  
  The slot number for a specific module.

#### Defaults

N/A.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Use the `slot/port` or `slot` parameter to display information for a specific port or for all ports on a specific module.
Examples

-> show lldp port 2/1/21 remote-system power-via-mdi

Chassis 00:04:a3:00:00:12, Port 00:04:a3:00:00:12:
  Remote ID = 12,
  MDI Power Support = Not Supported,
  MDI Power State = disabled,
  Pair Control Ability = not controllable,
  Power Pair = Alternative A,
  Power Class = Class4,
  Power Type = Type 1 PD,
  Power Source = PSE,
  Simultaneous Powering Both Modes = Supported,
  Power Priority = Low,
  PD Requested Power Value = 130,
  PSE Allocated Power Value = 130,
  PD Requested Power Value Mode A = 0,
  PSE Allocated Power Value ALT A = 0,
  PD Requested Power Value Mode B = 0,
  PSE Allocated Power Value ALT B = 0,
  PD Powered Status = Invalid,
  Dual-signature Class ext Mode A = Invalid,
  Dual-signature Class ext Mode B = Invalid,
  Power Class ext = Invalid,
  Power Demand Electrically Isolated = False,
  Power Type Ext = Type 3 PSE,
  Power Down Request = False,
  Power Down Time = 0

All Power Values are in 0.1W
### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote ID</td>
<td>The Index of the Remote Device.</td>
</tr>
<tr>
<td>MDI Power Support</td>
<td>Indicates if MDI power is supported.</td>
</tr>
<tr>
<td>MDI Power State</td>
<td>Indicates if the PSE function is enabled or disabled.</td>
</tr>
<tr>
<td>Pair Control Ability</td>
<td>Indicates if the PSE has the capability to control which PSE pin out</td>
</tr>
<tr>
<td></td>
<td>alternative is used for PD detection and power</td>
</tr>
<tr>
<td>Power Pair</td>
<td>Indicates the PSE power pair used to detect and supply power on both</td>
</tr>
<tr>
<td></td>
<td>pairsets.</td>
</tr>
<tr>
<td>Power Class</td>
<td>Indicates the power class used by the PD for transmission.</td>
</tr>
<tr>
<td>Power Type</td>
<td>Indicates the power type corresponding to the Type 2 PDs and PSEs.</td>
</tr>
<tr>
<td>Power Source</td>
<td>Indicates the power source (PD or PSE).</td>
</tr>
<tr>
<td>Simultaneous Powering Both</td>
<td>Indicates if the PD supports powering of both Modes simultaneously.</td>
</tr>
<tr>
<td>Modes</td>
<td></td>
</tr>
<tr>
<td>Power Priority</td>
<td>Indicates the priority of the power.</td>
</tr>
<tr>
<td>PD Requested Power Value</td>
<td>Indicates the maximum input average power the PD is requesting. The</td>
</tr>
<tr>
<td></td>
<td>power expressed in units of 0.1 W. The valid values for these bits are</td>
</tr>
<tr>
<td></td>
<td>decimal 0 through 999.</td>
</tr>
<tr>
<td>PSE Allocated Power Value</td>
<td>Indicates the maximum input average power the PSE expects the PD to</td>
</tr>
<tr>
<td></td>
<td>draw.</td>
</tr>
<tr>
<td>PD Requested Power Value</td>
<td>Indicates the maximum input average power level the PD is requesting</td>
</tr>
<tr>
<td>Mode A</td>
<td>for the Mode A. The power expressed in units of 0.1 W. The valid</td>
</tr>
<tr>
<td></td>
<td>values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PSE Allocated Power Value</td>
<td>Indicates the maximum input average power level, the PSE expects the</td>
</tr>
<tr>
<td>ALT A</td>
<td>dual-signature PD to draw on the Alternative A when the PSE provides</td>
</tr>
<tr>
<td></td>
<td>power over 4-pair. The power expressed in units of 0.1 W. The valid</td>
</tr>
<tr>
<td></td>
<td>values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PD Requested Power Value</td>
<td>Indicates the maximum input average power level the PD is requesting</td>
</tr>
<tr>
<td>Mode B</td>
<td>for the Mode B. The power expressed in units of 0.1 W. The valid</td>
</tr>
<tr>
<td></td>
<td>values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PSE Allocated Power Value</td>
<td>Indicates the maximum input average power level, the PSE expects the</td>
</tr>
<tr>
<td>ALT B</td>
<td>dual-signature PD to draw on the Alternative B when the PSE provides</td>
</tr>
<tr>
<td></td>
<td>power over 4-pair. The power expressed in units of 0.1 W. The valid</td>
</tr>
<tr>
<td></td>
<td>values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PD Powered Status</td>
<td>Indicates the existing powered configuration of the PD. The PD shall</td>
</tr>
<tr>
<td></td>
<td>set this field according to its signature configuration and the current</td>
</tr>
<tr>
<td></td>
<td>powering status.</td>
</tr>
<tr>
<td>Dual-signature Class ext Mode</td>
<td>Indicates the PSEs assigned Class for Alternative A.</td>
</tr>
<tr>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Dual-signature Class ext Mode</td>
<td>Indicates the PSEs assigned Class for Alternative B.</td>
</tr>
<tr>
<td>B</td>
<td></td>
</tr>
<tr>
<td>Power Class ext</td>
<td>Indicates the power class of the PD and PSE.</td>
</tr>
<tr>
<td>Power Demand Electrically</td>
<td>Indicates if the power demand on mode A and mode B is electrically</td>
</tr>
<tr>
<td>Isolated</td>
<td>isolated or not isolated. The value will be TRUE if isolated or FALSE</td>
</tr>
<tr>
<td></td>
<td>if not isolated.</td>
</tr>
<tr>
<td>Power Type Ext</td>
<td>Indicates the power type of the external supply.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Down Request</td>
<td>Indicates if the PD has a request to terminate the power delivery.</td>
</tr>
<tr>
<td>Power Down Time</td>
<td>Indicates the time duration the PD has requested to terminate the power</td>
</tr>
<tr>
<td></td>
<td>delivery. The duration is in seconds. If the value is 0, then it remains</td>
</tr>
<tr>
<td></td>
<td>unpowered. The valid range is 0 through 262143.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- **lldp tlv application** Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port.
- **lldp tlv application priority** Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.
- **show lldp config** Displays the general LLDP configuration information for LLDP ports.

**MIB Objects**

lldpXdot3RemPowerTable
   lldpRemLocalPortNum
   lldpXdot3RemPowerMDISupported
   lldpXdot3RemPowerMDIEnabled
   lldpXdot3RemPowerPairControlable
   lldpXdot3RemPowerPairs
   lldpXdot3RemPowerClass
   alaLldpXdot3RemPowerType
   alaLldpXdot3RemPowerSource
   alaLldpXdot3RemPowerPD4PID
   alaLldpXdot3RemPowerPriority
   alaLldpXdot3RemPDRequestedPowerValue
   alaLldpXdot3RemPSERequestedPowerValue
   alaLldpXdot3RemPDRequestedPowerValueA
   alaLldpXdot3RemPDRequestedPowerValueB
   alaLldpXdot3RemPSEAllocatedPowerValueA
   alaLldpXdot3RemPSEAllocatedPowerValueB
   alaLldpXdot3RemPDPoweredStatus
   alaLldpXdot3RemPowerPairsExt
   alaLldpXdot3RemPowerClassExt
   alaLldpXdot3RemPowerClassExtA
   alaLldpXdot3RemPowerClassExtB
   alaLldpXdot3RemPowerTypeExt
   alaLldpXdot3RemPDLoad
   alaLldpXdot3RemPSEMaxAvailPower
   alaLldpXdot3RemPowerDownRequest
   alaLldpXdot3RemPowerDownTime
show lldp remote-system power-via-mdi-measurements

Displays the information of remote system which includes the information received in the power via MDI measurements TLV. The measurements are electrical measurements.

```
show lldp [port chassis/slot/port[-port2] | slot chassis/slot] remote-system power-via-mdi-measurements
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **slot**
  - The slot number for a specific module.

### Defaults

N/A.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **slot/port** or **slot** parameter to display information for a specific port or for all ports on a specific module.

### Examples

```
-> show lldp port 2/1/21 remote-system power-via-mdi-measurements
```

Chassis <chassis-id>, Port <port-id>:

- Supported = Voltage|Current|Power|Energy,
- Valid = Voltage|Current|Power|Energy,
- Request = Voltage|Current|Power|Energy,
- Voltage Uncertainty = 20 mV,
- Current Uncertainty = 30 mA,
- Power Uncertainty = 50 mW,
- Energy Uncertainty = 100 kJ,
- Voltage Measurement = 30 mV,
- Current Measurement = 40 mA,
- Power Measurement = 100 mW,
- Energy Measurement = 200 kJ,
- Power Price Index = <>
output definitions

<table>
<thead>
<tr>
<th><strong>Supported</strong></th>
<th>Indicates the supported measurement (Voltage, Current, Power, Energy) by the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Valid</strong></td>
<td>Indicates which measurement field contains valid data.</td>
</tr>
<tr>
<td><strong>Request</strong></td>
<td>Indicates the type of measurement for request.</td>
</tr>
<tr>
<td><strong>Voltage Uncertainty</strong></td>
<td>Indicates the unit of expanded uncertainty for the voltage measurement. The units are measured in 1 mV. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td><strong>Current Uncertainty</strong></td>
<td>Indicates the unit of expanded uncertainty for the current measurement. The units are measured in 0.1 mA. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td><strong>Power Uncertainty</strong></td>
<td>Indicates the unit of expanded uncertainty for the power measurement. The units are measured in 10 mW. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td><strong>Energy Uncertainty</strong></td>
<td>Indicates the unit of expanded uncertainty for the energy measurement. The units are measured in 0.1 kJ. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td><strong>Voltage Measurement</strong></td>
<td>Indicates the measurement of the pairset with the highest voltage. Measured in units of 1 mV.</td>
</tr>
<tr>
<td><strong>Current Measurement</strong></td>
<td>Indicates the current measurement. Expressed in units of 0.1 mA. The valid units are 0 through 20000.</td>
</tr>
<tr>
<td><strong>Power Measurement</strong></td>
<td>Indicates the power measurement. Expressed in units of 10 mW. The valid units are 0 through 10000.</td>
</tr>
<tr>
<td><strong>Energy Measurement</strong></td>
<td>Indicates the energy measurement. Expressed in units of 0.1 kJ since power on. The valid units are 0 through 4294967295.</td>
</tr>
<tr>
<td><strong>Power Price Index</strong></td>
<td>Indicates the current price of electricity compared to what the PSE considers the nominal electricity price. The determination of the nominal electricity price is implementation dependent. The PSE sets the value of this field taking the availability of power from any external and internal resources, and the relative supply and demand balance, into account. A value of 0xFFFF means that no power price index is available.</td>
</tr>
</tbody>
</table>

The valid values for these bits are decimal 0 through 65000, and hexadecimal value 0xFFFF.

Release History

Release 7.3.2; command introduced.
**Related Commands**

**lldp tlv application**
Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port.

**lldp tlv application priority**
Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

**show lldp config**
Displays the general LLDP configuration information for LLDP ports.

**MIB Objects**

<table>
<thead>
<tr>
<th>Object Path</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldpXdot3RemPowerMeasurementsTable</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasVoltageSupport</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasCurrentSupport</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasPowerSupport</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasEnergySupport</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasVoltageRequest</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasCurrentRequest</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasPowerRequest</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasEnergyRequest</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasVoltageValid</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasCurrentValid</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasPowerValid</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasurementSource</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasVoltageUncertainty</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasCurrentUncertainty</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasPowerUncertainty</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemMeasEnergyUncertainty</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemVoltageMeasurement</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemCurrentMeasurement</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemPowerMeasurement</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemEnergyMeasurement</td>
<td></td>
</tr>
<tr>
<td>alaLldpXdot3RemPSEPowerPriceIndex</td>
<td></td>
</tr>
</tbody>
</table>
show lldp local-port power-via-mdi

Displays the information of the local system which includes the information transmitted in the power via MDI.

show lldp [port chassis/slot/port[-port2] | slot chassis/slot] local-port power-via-mdi

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port[-port2]</td>
<td>The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).</td>
</tr>
<tr>
<td>slot</td>
<td>The slot number for a specific module.</td>
</tr>
</tbody>
</table>

Defaults

N/A.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the slot/port or slot parameter to display information for a specific port or for all ports on a specific module.
**Examples**

--> show lldp port 1/1/17 local-port power-via-mdi

Local Port 1/1/17 LLDP Power VIA MDI Info:

- MDI Power Support = Supported,
- MDI Power State = enabled,
- Pair Control Ability = not controllable,
- Power Pair = Alternative A,
- Power Class = Class2,
- Power Type = Type 2 PSE,
- Power Source = Primary Power Source,
- Power Priority = Low,
- PD Requested Power Value = 0,
- PSE Allocated Power Value = 64,
- PD Requested Power Value Mode A = 0,
- PSE Allocated Power Value ALT A = 64,
- PD Requested Power Value Mode B = 0,
- PSE Allocated Power Value ALT B = 0,
- PSE Powering Status = 2 Pair,
- PSE Power Pair Ext = Alt A,
- Dual-signature Class Ext Mode A = Single Signature,
- Dual-signature Class Ext Mode B = Single Signature,
- Power Class Ext = Class2,
- Power Type Ext = Type 3 PSE,
- Maximum Available Power = 64,
- Auto Class = Not Supported
- Auto Class Completion Status = Idle

All Power Values are in 0.1W
**output definitions**

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote ID</td>
<td>The Index of the Remote Device.</td>
</tr>
<tr>
<td>MDI Power Support</td>
<td>Indicates if MDI power is supported.</td>
</tr>
<tr>
<td>MDI Power State</td>
<td>Indicates if the PSE function is enabled or disabled.</td>
</tr>
<tr>
<td>Pair Control Ability</td>
<td>Indicates if the PSE has the capability to control which PSE pin out alternative is used for PD detection and power</td>
</tr>
<tr>
<td>Power Pair</td>
<td>Indicates the PSE power pair used to detect and supply power on both pairsets.</td>
</tr>
<tr>
<td>Power Class</td>
<td>Indicates the power class used by the PD for transmission.</td>
</tr>
<tr>
<td>Power Type</td>
<td>Indicates the power type corresponding to the Type 2 PDs and PSEs.</td>
</tr>
<tr>
<td>Power Source</td>
<td>Indicates the power source (PD or PSE).</td>
</tr>
<tr>
<td>Simultaneous Powering Both Modes</td>
<td>Indicates if the PD supports powering of both Modes simultaneously.</td>
</tr>
<tr>
<td>Power Priority</td>
<td>Indicates the priority of the power.</td>
</tr>
<tr>
<td>PD Requested Power Value</td>
<td>Indicates the maximum input average power the PD is requesting. The power expressed in units of 0.1 W. The valid values for these bits are decimal 0 through 999.</td>
</tr>
<tr>
<td>PSE Allocated Power Value</td>
<td>Indicates the maximum input average power the PSE expects the PD to draw.</td>
</tr>
<tr>
<td>PD Requested Power Value Mode A</td>
<td>Indicates the maximum input average power level the PD is requesting for the Mode A. The power expressed in units of 0.1 W. The valid values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PSE Allocated Power Value ALT A</td>
<td>Indicates the maximum input average power level, the PSE expects the dual-signature PD to draw on the Alternative A when the PSE provides power over 4-pair. The power expressed in units of 0.1 W. The valid values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PD Requested Power Value Mode B</td>
<td>Indicates the maximum input average power level the PD is requesting for the Mode B. The power expressed in units of 0.1 W. The valid values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PSE Allocated Power Value ALT B</td>
<td>Indicates the maximum input average power level, the PSE expects the dual-signature PD to draw on the Alternative B when the PSE provides power over 4-pair. The power expressed in units of 0.1 W. The valid values for these bits are decimal 0 through 499.</td>
</tr>
<tr>
<td>PD Powered Status</td>
<td>Indicates the existing powered configuration of the PD. The PD shall set this field according to its signature configuration and the current powering status.</td>
</tr>
<tr>
<td>Dual-signature Class ext Mode A</td>
<td>Indicates the PSEs assigned Class for Alternative A.</td>
</tr>
<tr>
<td>Dual-signature Class ext Mode B</td>
<td>Indicates the PSEs assigned Class for Alternative B.</td>
</tr>
<tr>
<td>Power Class ext</td>
<td>Indicates the power class of the PD and PSE.</td>
</tr>
<tr>
<td>Power Demand Electrically Isolated</td>
<td>Indicates if the power demand on mode A and mode B is electrically isolated or not isolated. The value will be TRUE if isolated or FALSE if not isolated.</td>
</tr>
<tr>
<td>Power Type Ext</td>
<td>Indicates the power type of the external supply.</td>
</tr>
</tbody>
</table>
The command `show lldp local-port power-via-mdi` is used to display information about the power supplied to a device via MDI. This command is useful for monitoring power usage and ensuring that devices are receiving the correct amount of power.

### Release History

Release 7.3.2; command introduced.

### Related Commands

- **lldp tlv application** Configures the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDU for the specified port.

- **lldp tlv application priority** Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

- **show lldp config** Displays the general LLDP configuration information for LLDP ports.

### MIB Objects

- **lldpXdot3LocPowerTable**
  - **lldpLocPortNum**
  - **lldpXdot3LocPowerPortClass**
  - **lldpXdot3LocPowerMDISupported**
  - **lldpXdot3LocPowerMDIEnabled**
  - **lldpXdot3LocPowerPairControlable**
  - **lldpXdot3LocPowerPairs**
  - **lldpXdot3LocPowerClass**
  - **alaLldpXdot3LocPowerType**
  - **alaLldpXdot3LocPowerSource**
  - **alaLldpXdot3LocPD4PID**
  - **alaLldpXdot3LocPowerPriority**
  - **alaLldpXdot3LocPDRRequestedPowerValue**
  - **alaLldpXdot3LocPSEAllocatedPowerValue**
  - **alaLldpXdot3LocPDRRequestedPowerValueA**
  - **alaLldpXdot3LocPSEAllocatedPowerValueA**
  - **alaLldpXdot3LocPSEAllocatedPowerValueB**
  - **alaLldpXdot3LocPSEPoweringStatus**
  - **alaLldpXdot3LocPDPoweredStatus**
  - **alaLldpXdot3LocPowerPairsExt**
  - **alaLldpXdot3LocPowerClassExtA**
  - **alaLldpXdot3LocPowerClassExtB**
  - **alaLldpXdot3LocPowerTypeExt**
  - **alaLldpXdot3LocPDLoad**
  - **alaLldpXdot3LocPSEMaxAvailPower**
  - **alaLldpXdot3LocPSEAutoClassSupport**

### Maximum Available Power

Indicates the highest power the PSE can grant. The PSE sets the value of this field taking available power budget and hardware capabilities into account. When connected to a dual-signature PD this value refers to the total amount of power available at the PI, even though power is allocated separately on a per pairset basis. A PD shall set this field to 0. Power expressed in units of 0.1 W. Valid values for these bits are 1 through 999.

### Auto Class

Indicates if the PSE supports or not supports auto class.

### Auto Class Completion Status

Indicates the status of the auto class measurement.
show lldp local-port power-via-mdi

alaLldpXdot3LocPowerDownRequest
alaLldpXdot3LocPowerDownTime
show lldp local-port power-via-mdi-measurements

Displays the information of the local system which includes the information transmitted in the power via MDI measurements. The measurements are electrical measurements.

show lldp [port chassis/slot/port[-port2] | slot chassis/slot] local-port power-via-mdi-measurements

Syntax Definitions

chassis
The chassis identifier.

slot/port[-port2]
The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

slot
The slot number for a specific module.

Defaults
N/A.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the slot/port or slot parameter to display information for a specific port or for all ports on a specific module.

Examples

-> show lldp port 1/1/17 local-port power-via-mdi-measurements
Local Port 1/1/17 LLDP Power VIA MDI Measurement Info:
Supported = Voltage|Current|Power|Energy,
Valid = Voltage|Current|Power|Energy,
Request = ,
Voltage Uncertainty = 5129 mV,
Current Uncertainty = 626 mA,
Power Uncertainty = 3410 mW,
Energy Uncertainty = 3 kJ,
Voltage Measurement = 5400 mV,
Current Measurement = 660 mA,
Power Measurement = 3600 mW,
Energy Measurement = 3 kJ,
Power Price Index = 0
802.1AB Commands

show lldp local-port power-via-mdi-measurements

**output definitions**

<table>
<thead>
<tr>
<th>Supported</th>
<th>Indicates the supported measurement (Voltage, Current, Power, Energy) by the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Indicates which measurement field contains valid data.</td>
</tr>
<tr>
<td>Request</td>
<td>Indicates the type of measurement for request.</td>
</tr>
<tr>
<td>Voltage Uncertainty</td>
<td>Indicates the unit of expanded uncertainty for the voltage measurement. The units are measured in 1 mV. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td>Current Uncertainty</td>
<td>Indicates the unit of expanded uncertainty for the current measurement. The units are measured in 0.1 mA. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td>Power Uncertainty</td>
<td>Indicates the unit of expanded uncertainty for the power measurement. The units are measured in 10 mW. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td>Energy Uncertainty</td>
<td>Indicates the unit of expanded uncertainty for the energy measurement. The units are measured in 0.1 kJ. The valid range is 1 through 65000.</td>
</tr>
<tr>
<td>Voltage Measurement</td>
<td>Indicates the measurement of the pairset with the highest voltage. Measured in units of 1 mV.</td>
</tr>
<tr>
<td>Current Measurement</td>
<td>Indicates the current measurement. Expressed in units of 0.1 mA. The valid units are 0 through 20000.</td>
</tr>
<tr>
<td>Power Measurement</td>
<td>Indicates the power measurement. Expressed in units of 10 mW. The valid units are 0 through 10000.</td>
</tr>
<tr>
<td>Energy Measurement</td>
<td>Indicates the energy measurement. Expressed in units of 0.1 kJ since power on. The valid units are 0 through 4294967295.</td>
</tr>
<tr>
<td>Power Price Index</td>
<td>Indicates the current price of electricity compared to what the PSE considers the nominal electricity price. The determination of the nominal electricity price is implementation dependent. The PSE sets the value of this field taking the availability of power from any external and internal resources, and the relative supply and demand balance, into account. A value of 0xFFFF means that no power price index is available.</td>
</tr>
</tbody>
</table>

The valid values for these bits are decimal 0 through 65000, and hexadecimal value 0xFFFF.

**Release History**

Release 7.3.2; command introduced.
**Related Commands**

**lldp tlv application**  Configure the switch to include the LLDP-DCBx Application Priority TLV in the LLDPDUs for the specified port.

**lldp tlv application priority**  Configures the LLDP-DCBx Application Priority TLV to advertise an 802.1p priority value for specific protocols on the specified port.

**show lldp config**  Displays the general LLDP configuration information for LLDP ports.

**MIB Objects**

```plaintext
lldpXdot3LocPowerMeasurementsTable
    lldpLocPortNum
    alaLldpXdot3LocMeasVoltageSupport
    alaLldpXdot3LocMeasCurrentSupport
    alaLldpXdot3LocMeasPowerSupport
    alaLldpXdot3LocMeasEnergySupport
    alaLldpXdot3LocMeasVoltageRequest
    alaLldpXdot3LocMeasCurrentRequest
    alaLldpXdot3LocMeasPowerRequest
    alaLldpXdot3LocMeasEnergyRequest
    alaLldpXdot3LocMeasVoltageValid
    alaLldpXdot3LocMeasCurrentValid
    alaLldpXdot3LocMeasPowerValid
    alaLldpXdot3LocMeasEnergyValid
    alaLldpXdot3LocMeasurementSource
    alaLldpXdot3LocMeasVoltageUncertainty
    alaLldpXdot3LocMeasCurrentUncertainty
    alaLldpXdot3LocMeasPowerUncertainty
    alaLldpXdot3LocMeasEnergyUncertainty
    alaLldpXdot3LocVoltageMeasurement
    alaLldpXdot3LocCurrentMeasurement
    alaLldpXdot3LocPowerMeasurement
    alaLldpXdot3LocEnergyMeasurement
    alaLldpXdot3LocPSEPowerPriceIndex
```
show lldp agent-destination-address

Displays the destination address of each agent.

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show lldp agent-destination-address
Lldp Agent                Name                     MAC address
-------------------------+----------------+------------------------
1  Nearest-Bridge         00-80-C2-00-00-0E
2  Non-TPMR-Bridge        Tcp/Sctp                  00-80-C2-00-00-03
3  Nearest-Customer-Bridge 00-80-C2-00-00-00
```

**output definitions**

- **Lldp Agent**
  - The LLDP agent identifier.
- **Name**
  - The name of the LLDP agent.
- **Destination MAC address**
  - The destination MAC address of the LLDP agent.

**Release History**

Release 7.3.1; command introduced.
**Related Commands**

**lldp lldpdu**

Specifies the switch to control the transmission and the reception of LLDPDUs for a particular chassis, slot, or port.

**MIB Objects**

- `lldpV2DestAddressTable`
  - `lldpV2AddressTableIndex`
  - `lldpV2DestMacAddress`
**lldp trust-agent**

Enables or disables the security mechanism globally (chassis level) or for a slot or a single port. By enabling LLDP security mechanism on a port, LLDP CMM task brings the LLDP status of the port as trusted and monitors the port for any LLDP security violation.

```
lldp {chassis/slot/port | chassis/slot | chassis} trust-agent [admin-state] {enable | disable} [chassis-id-subtype {chassis-component | interface-alias | port-component | mac-address | network-address | interface-name | locally-assigned | any}]
```

**Syntax Definitions**

- `chassis/slot/port`: The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).
- `chassis/slot`: The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).
- `chassis`: Specifies all the ports in the chassis.
- `enable`: Enables LLDP security mechanism.
- `disable`: Disables LLDP security mechanism.
- `chassis-component`: The chassis component is used for validating the remote agent.
- `interface-alias`: The alias configured for the interface is used for validating the remote agent.
- `port-component`: The port component is used for validating the remote agent.
- `mac-address`: The MAC address is used for validating the remote agent.
- `network-address`: The network address is used for validating the remote agent.
- `interface-name`: The interface name is used for validating the remote agent.
- `locally-assigned`: The locally assigned component is used for validating the remote agent, that is the chassis information, which can be locally assigned (the local configuration).
- `any`: The remote agent with any chassis ID sub type is accepted as a trust agent.

**Defaults**

- `'any'`: If the chassis ID sub type is not configured for validating the remote agent, by default, the first remote agent is accepted as a trust agent considering any of the chassis ID sub types.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- By enabling security on chassis/slot level, the ports that come under the respective level are monitored for any LLDP security violation.

- If the chassis ID sub type is not configured for validating the remote agent, then the LLDP learns the first remote agent with available chassis ID TLV (Time, Length, Value) received in the PDU.

- After a link up is received on a LLDP security enabled port, LLDP CMM waits for three times the LLDP timer interval (30 seconds). If no LLDP PDU is received after link up that has no remote agent, the port is moved to a violation state.

- If a trusted remote agent already exists, and if no LLDP remote agent is learned even after three times the LLDP timer interval (30 seconds), the port is moved to a violation state. If a new LLDP remote agent is learned after the link toggle, then the port is moved to a violation state.

- If the same chassis ID and port ID already exist in the trusted remote agent database but on a different port, then the port remote agent is learned and the port is moved to a violation state. If a new LLDP remote agent is learned on a port that has a trusted LLDP remote agent, then the port is moved to a violation state.

**Examples**

- `lldp chassis trust-agent admin-state enable`
- `lldp chassis trust-agent chassis-id-subtype chassis-component`

**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `lldp trust-agent violation-action` Sets the action to be performed when a violation is detected.
- `show lldp trusted remote-agent` Displays information on trusted remote-agents.
- `show lldp trust-agent` Displays information on local LLDP agent or port.

**MIB Objects**

- `alaLldpTrustAdminStatus`  
- `alaLldpTrustChassisIdSubType`
lldp trust-agent violation-action

Sets the action to be performed when a violation is detected.

```
lldp {chassis/slot/port | chassis/slot | chassis} trust-agent violation-action {trap-and-shutdown | trap | shutdown}
```

**Syntax Definitions**

- `chassis/slot/port`  
  The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).

- `chassis/slot`  
  The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).

- `chassis`  
  All switch ports.

- `trap-and-shutdown`  
  Shuts down the port and sends a trap notification when a violation is detected.

- `trap`  
  Sends a trap notification when a violation is detected.

- `shutdown`  
  Shuts down the port when a violation is detected.

**Defaults**

By default, trust agent violation action is set to ‘trap’.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the port is in a shutdown state, clear the violation on the port by using the command “`interfaces chassis/slot/port1-port2] clear-violation-all`”

- Clearing the violation on a port does not clear the trusted remote agent existing on that port. To clear the trusted remote agent, disable the LLDP security mechanism on the port.

- If the port is in a shutdown state due to violation and the port link is toggled, only the link goes up. The port still remains in the violation state and the trusted remote agent existing on that port is not cleared.

**Examples**

- `lldp chassis trust-agent violation-action trap`
- `lldp slot 3 trust-agent violation-action shutdown`
Release History

Release 8.3.1; command introduced.

Related Commands

lldp trust-agent
Sets the status of trust admin status for a port.

show lldp trusted remote-agent
Displays information on trusted remote-agents.

show lldp trust-agent
Displays information on local LLDP agent or port.

MIB Objects

alaLldpTrustAction
show lldp trusted remote-agent

Displays information on trusted remote-agents.

```
show lldp [chassis/slot | chassis/slot/port] trusted remote-agent
```

**Syntax Definitions**

- `chassis/slot`: The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).
- `chassis/slot/port`: The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the slot/port or slot parameter to display information for a specific port or for all ports on a specific module.
- LLDP trust agent must be enabled globally on the chassis or individually on a port in order to get the `show lldp trusted remote-agent` command output.

**Examples**

```
-> lldp chassis trust-agent enable
-> lldp chassis trust-agent chassis-id-subtype mac-address

-> show lldp trusted remote-agent
```

```
Trusted Remote LLDP Agents on Local Slot/Port: 1/7
Chassis ID Subtype = 4 (MAC Address),
Chassis ID = 00:e0:b1:7a:e6:3c,
Port ID Subtype = 7 (Locally assigned),
Port ID = 1017
```
output definitions

<table>
<thead>
<tr>
<th>Trusted Remote LLDP Agents on Local Slot/Port</th>
<th>The slot number to which the remote trusted agent is associated and the physical port number on that module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis ID Subtype</td>
<td>The sub type that describes the chassis ID.</td>
</tr>
<tr>
<td>Chassis ID</td>
<td>The chassis ID (MAC address).</td>
</tr>
<tr>
<td>Port ID Subtype</td>
<td>The sub type that describes port ID.</td>
</tr>
<tr>
<td>Port ID</td>
<td>The port ID (Port MAC).</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command introduced.

Related Commands

- `lldp trust-agent`             Sets the status of trust admin status for a port.
- `lldp trust-agent violation-action` Sets the action to be performed when a violation is detected.
- `show lldp trust-agent`        Displays information on local LLDP agent/port.

MIB Objects

- N/A
show lldp trust-agent

Displays information of the local LLDP agent or port.

show lldp [chassis/slot | chassis/slot/port] trust-agent

Syntax Definitions

chassis/slot
The chassis ID and slot number for the module (for example, 1/2 specifies chassis 1, slot 2).

chassis/slot/port
The chassis ID, slot, and port number for the module and the physical port number on that module (for example, 1/2/4 specifies chassis 1, port 4 on slot 2).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the slot/port or num (slot number) values to display information for a specific port or for all ports on a specific module.
- LLDP trust agent must be enabled globally on the chassis or individually on a port in order to get the show lldp trust-agent command output correctly.
- If LLDP security is disabled this command correctly displays the ‘Admin Status’ as ‘Disabled’; however the other output parameters will display their default values.

Examples

-> lldp chassis trust-agent enable
-> lldp chassis trust-agent chassis-id-subtype chassis-component

-> show lldp trust-agent

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Admin Status</th>
<th>Violation Action</th>
<th>Violation Status</th>
<th>Chassis Subtype</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>Enabled</td>
<td>Trap Only</td>
<td>Trusted</td>
<td>1(Chassis Component)</td>
</tr>
<tr>
<td>1/2</td>
<td>Enabled</td>
<td>Trap Only</td>
<td>Trusted</td>
<td>1(Chassis Component)</td>
</tr>
<tr>
<td>1/3</td>
<td>Enabled</td>
<td>Trap Only</td>
<td>Trusted</td>
<td>1(Chassis Component)</td>
</tr>
<tr>
<td>1/4</td>
<td>Disabled</td>
<td>Shutdown</td>
<td>Violated</td>
<td>1(Chassis Component)</td>
</tr>
</tbody>
</table>
802.1AB Commands

1/5  Enabled  Shutdown  Trusted  1(Chassis Component)
1/6  Enabled  Trap-and-Shutdown  Trusted  1(Chassis Component)
1/7  Disabled  Trap-and-Shutdown  Violated  1(Chassis Component)
1/8  Enabled  Trap Only  Trusted  1(Chassis Component)
1/9  Enabled  Trap Only  Trusted  1(Chassis Component)
1/10  Enabled  Trap Only  Trusted  1(Chassis Component)

output definitions

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>The LLDP slot and port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>Indicates the administrative status of the LLDP port, Enabled or Disabled</td>
</tr>
<tr>
<td>Violation Action</td>
<td>Indicates the action performed when a violation is detected. The options are - Trap Only, Trap-and-Shutdown, and Shutdown Only.</td>
</tr>
<tr>
<td>Violation Status</td>
<td>The violation status of the port, Trusted or Violated</td>
</tr>
<tr>
<td>Chassis Subtype</td>
<td>The sub type that describes the chassis ID.</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command introduced.

Related Commands

lldp trust-agent
lldp trust-agent violation-action
show lldp trusted remote-agent

MIB Objects

N/A
SIP Snooping feature address the key challenge of real time delivery and monitoring requirements for media streams from SIP devices. SIP snooping feature provides plug and play support to the device, where it automatically identifies the ports used. It also enhances the security of device.

SIP Snooping prioritizes voice and video traffic over non-voice traffic. To summarize, SIP Snooping:

- Identifies and marks the SIP and its corresponding media streams. Each media stream contains Real Time Protocol (RTP) and Real Time Control Protocol (RTCP) flows. Marking is done using the DSCP field in the IP header.
- Provides user configured QOS treatment for SIP/RTP/RTCP traffic flows based on its marking.
- Also snoops voice quality metrics of media streams from their RTCP packets and displays them to the user with knowledge of media reception quality in real time and helps to diagnose the problems on their quality. Also in addition, trap will be generated when voice quality parameters like Jitter, Round trip time, Packet-lost, R-factor and MOS values of media streams crosses user configured threshold.

This chapter includes SIP commands and their descriptions.

MIB information for SIP commands is as follows:

- **Filename**: ALCATEL-IND1-SIP-SNOOPING-MIB.mib
- **Module**: aluSIPSnoopingMIB

A summary of the available commands is listed here:

- sip-snooping admin-state
- sip-snooping port admin-state
- sip-snooping mode
- sip-snooping trusted server
- sip-snooping sip-control
- sip-snooping sos-call number
- sip-snooping sos-call dscp
- sip-snooping udp port
- sip-snooping tcp port
- sip-snooping threshold
- sip-snooping logging-threshold num-of-calls
- show sip-snooping call-records
- clear sip-snooping statistics
- show sip-snooping config
- show sip-snooping ports
- show sip-snooping statistics
- show sip-snooping registered-clients
sip-snooping admin-state

Enables or disables the SIP snooping on the switch.

`sip-snooping admin-state {enable | disable}`

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables SIP snooping</td>
</tr>
<tr>
<td>disable</td>
<td>Disables SIP snooping</td>
</tr>
</tbody>
</table>

### Defaults

By default, SIP-snooping is disabled on the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If SIP snooping is disabled at the port level, enabling SIP snooping globally will not override the configuration of that port.
- If SIP snooping is disabled and enabled, it is mandatory that the phones re-register for successful DSCP marking.

### Examples

- `-> sip-snooping admin-state enable`
- `-> sip-snooping admin-state disable`

### Release History

Release 8.1.1; command was introduced.
**Related Commands**

- **sip-snooping port admin-state**  
  Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate of ports.

- **show sip-snooping ports**  
  Shows the SIP snooping port level data.

- **show sip-snooping config**  
  Shows the configuration done for SIP snooping.

**MIB Objects**

- **aluSIPSnoopingStatus**
**sip-snooping port admin-state**

Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate.

```
sip-snooping {port chassis/slot/port[-port2] | linkagg agg_num} admin-state {enable | disable}
```

### Syntax Definitions

- `chassis/slot/port[-port2]` The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
- `agg_num` A link aggregate ID number.
- `enable` Enables SIP snooping to mirror all SIP PDU that ingress on that port.
- `disable` Disables SIP snooping and will not mirror SIP PDU that ingress on that port.

### Defaults

By default, SIP snooping is disabled on the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use this command for port/linkagg level SIP Snooping configuration on the switch.
- SIP snooping must be enabled globally to activate port/linkagg level configuration.
- Even after SIP snooping is globally disabled, port/linkagg level configuration is saved. This configuration will be used when SIP snooping is enabled globally again.
- Port level configuration is not allowed on a member port of a linkagg.
- If a port joins a linkagg, port level configuration is overridden by the linkagg configuration. Port level configuration will be activated if the port leaves the linkagg.

### Examples

```
-> sip-snooping port 1/1/5-6 admin-state enable
-> sip-snooping linkagg 1 admin-state enable
```

### Release History

Release 8.1.1; command was introduced.
Related Commands

show sip-snooping ports  Shows the SIP snooping port level data.

MIB Objects

aluSIPSnoopingSlotPortIndex
  aluSIPSnoopingRowStatus
sip-snooping mode

Configures the SIP snooping mode for the specified port or link aggregate.

```
```

**Syntax Definitions**

- `chassis/slot/port[1-2]` The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
- `agg_num` The link aggregate ID number.
- `force-edge` Media TCAM entries to be created for dialogs that transverse the specific port.
- `force-non-edge` No Media TCAM entries for dialogs that transverse the specific port.
- `automatic` Sets to default mode. The port’s edge/non-edge mode is derived by the switch/router based on LLDP received or not on the port.

**Defaults**

By default, the SIP snooping mode is set to automatic.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command for port/linkagg level SIP Snooping configuration on the switch.
- Force-edge-port/force-non-edge port option to overwrite default port mode learned by either received or not received switch/router capability through LLDP.
- Port level configuration is not allowed on a member port of a linkagg.
- If a port joins a linkagg, port level configuration is overridden by linkagg configuration. Port level configuration will be activated if it leaves the linkagg.

**Examples**

- `-> sip-snooping port 1/1/5-6 mode force-edge`
- `-> sip-snooping linkagg 1 mode force-non-edge`
**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `show sip-snooping ports` Shows the SIP snooping port level data.

**MIB Objects**

aluSIPSnoopingSlotPortIndex

aluSIPSnoopingPortConfigPortMode
**sip-snooping trusted server**

Configure the IP addresses of the trusted servers on a switch.

```
sip-snooping trusted-server [ip_address1 ip_address2 ip_address ...ip_address8]
```

```
no sip-snooping trusted-server {ip_address | all}
```

---

**Syntax Definitions**

- `ip_address1[-ip_address2]` The IP address of one or more trusted servers.
- `all` Specifies all the IP addresses.

**Defaults**

By default, no trusted servers are configured. All SIP based calls using any call server will be supported.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is used to configure the IP addresses of the trusted servers. If a trusted server is configured, then only the calls initiated through those servers will be supported.
- A maximum of 8 trusted servers can be configured.
- If no trust servers are configured, all SIP based calls using any call server will be supported.
- Use the `no` form of the command to remove any trusted IP or all trusted IP addresses.

**Examples**

- `-> sip-snooping trusted-server 192.254.32.22 192.254.32.33`
- `-> no sip-snooping trusted-server 192.254.32.22`
- `-> no sip-snooping trusted-server all`

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `show sip-snooping config` Shows the configuration done for SIP snooping.
**MIB Objects**

aluSIPSnoopingSIPTrustedServerIPAddress1
aluSIPSnoopingSIPTrustedServerIPAddress2
aluSIPSnoopingSIPTrustedServerIPAddress3
aluSIPSnoopingSIPTrustedServerIPAddress4
aluSIPSnoopingSIPTrustedServerIPAddress5
aluSIPSnoopingSIPTrustedServerIPAddress6
aluSIPSnoopingSIPTrustedServerIPAddress7
aluSIPSnoopingSIPTrustedServerIPAddress8
**sip-snooping sip-control**

Configures SIP control DSCP marking.

```
sip-snooping sip-control dscp num
sip-snooping sip-control no dscp
```

**Syntax Definitions**

`num` The DSCP number. The valid range is 1–4 Mbps.

**Defaults**

By default no marking/prioritizing or rate limit is performed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- This command is used for the SIP control DSCP marking. A built-in rate limiter of 1 Mbps is configured to rate limit SIP PDUs being marked by the switch.

- The packet gets its priority as normal packet, either from the QoS port configuration (trust the packet DSCP or untrusted) or from a user configured QoS policy.

- Use `no` form of the command is to set default mode.

**Examples**

```
-> sip-snooping sip-control dscp 40
-> sip-snooping sip-control no dscp
```

**Release History**

Release 8.1.1; command was introduced.
Related Commands

**show sip-snooping config**  
Shows the configuration done for SIP snooping.

MIB Objects

aluSIPSnoopingSIPControlDSCP
**sip-snooping sos-call number**

Configures the SOS call strings in SIP snooping.

```
sip-snooping sos-call number string1 string2 ... string4

no sip-snooping sos-call number {string | all}
```

**Syntax Definitions**

- `string1 ... string4`: Specifies the SOS call string.
- `all`: Specifies all the SOS call strings.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is used for the configuration of the SOS call strings. A maximum of 4 SOS call strings can be configured for an exact match on the “to” URI (user part only).
- No support of regular expression. If no string is specified, no SOS call can be identified in the system.
- Use `no` form of this command to remove existing SOS call strings.

**Examples**

```
-> sip-snooping sos-call number "911" "2233"
-> no sip-snooping sos-call number "911"
-> no sip-snooping sos-call number all
```

**Release History**

Release 8.1.1; command was introduced.
Related Commands

`show sip-snooping config` Displays the SIP snooping configuration.

MIB Objects

aluSIPSnoopingSOSCallNumber1
aluSIPSnoopingSOSCallNumber2
aluSIPSnoopingSOSCallNumber3
aluSIPSnoopingSOSCallNumber4
sip-snooping sos-call dscp

Configures the SOS-Call RTP/RTCP DSCP marking.

**sip-snooping sos-call dscp num**

### Syntax Definitions

**num**

Specifies the DSCP number.

### Defaults

The default configuration is 46 EF.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 8.1.1; command was introduced.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is used for the configuration of the SOS-Call RTP/RTCP DSCP marking. A built-in rate limiter of 128 kbps is configured to rate limit a uni-direction media stream being marked by the switch.

- SOS calls are identified only for the Audio media type. All other media type calls are considered normal calls.

### Examples

-> sip-snooping sos-call dscp 56

### Release History

Release 8.1.1; command was introduced.

### Related Commands

**show sip-snooping config**

Displays the SIP snooping configuration for the switch.

### MIB Objects

aluSIPSnoopingSOSCallRTPDSCP
sip-snooping udp port

Configures the UDP port for SIP Snooping.

**sip-snooping udp-port** `udp-port1` `udp-port 2` ... `udp-port 8`

no sip-snooping udp-port `{udp-port | all}`

---

**Syntax Definitions**

- `udp-port 1` ... `udp-port 8`: Specifies the UDP port for SIP snooping.
- `all`: Specifies all the UDP ports designated for SIP snooping.

**Defaults**

By default no UDP ports and SIP mirroring is performed with the method name and SIP2.0 strings.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A maximum of 8 UDP ports can be configured on a switch.
- Use **no** form of this command to remove any UDP port configured earlier.

**Examples**

- `-> sip-snooping udp-port 5260 5060`
- `-> no sip-snooping udp-port 5260`
- `-> no sip-snooping udp-port all`

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `show sip-snooping config`: Shows the configuration done for SIP snooping.
MIB Objects

aluSIPSnoopingSIPUDPPort1
aluSIPSnoopingSIPUDPPort2
aluSIPSnoopingSIPUDPPort3
aluSIPSnoopingSIPUDPPort4
aluSIPSnoopingSIPUDPPort5
aluSIPSnoopingSIPUDPPort6
aluSIPSnoopingSIPUDPPort7
aluSIPSnoopingSIPUDPPort8
**sip-snooping tcp port**

Configures the Server listening TCP ports for SIP Snooping.

```
sip-snooping tcp-port tcp-port1 tcp-port2 ... tcp-port8
no sip-snooping tcp-port {tcp-port | all}
```

---

**Syntax Definitions**

```
tcp-port1 ... tcp-port8
all
```

- `tcp-port1 ... tcp-port8`: Specifies the TCP port for SIP snooping.
- `all`: Specifies all the SOS call strings.

---

**Defaults**

By default, TCP port is 5260.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- A maximum of 8 TCP ports can be configured on a switch.
- The default port will be overwritten if the user configures any other port.
- Use the `no` form of this command to remove any TCP port configured earlier.

---

**Examples**

```
-> sip-snooping tcp-port 5260 5060
-> no sip-snooping tcp-port 5260
-> no sip-snooping tcp-port all
```

---

**Release History**

Release 8.1.1; command was introduced.

---

**Related Commands**

- `show sip-snooping config`: Shows the configuration done for SIP snooping.
MIB Objects

aluSIPSnoopingSIPTCPPort1
aluSIPSnoopingSIPTCPPort2
aluSIPSnoopingSIPTCPPort3
aluSIPSnoopingSIPTCPPort4
aluSIPSnoopingSIPTCPPort5
aluSIPSnoopingSIPTCPPort6
aluSIPSnoopingSIPTCPPort7
aluSIPSnoopingSIPUDPPort8
**sip-snooping threshold**

Configure the various thresholds of SIP snooping.

```
sip-snooping threshold {audio | video | other} {jitter jitter_ms_num | packet-lost % num | round-trip-delay round_trip_delay_ms_num | r-factor rfactor_num | mos mos_num}
```

### Syntax Definitions

- `audio` Specify threshold for audio.
- `video` Specify threshold for video.
- `other` Specify threshold for other.
- `jitter_ms_num` Specify jitter in milliseconds. The valid range is 0–300.
- `% num` Specify packet lost in percentage. The valid range is 0–99%.
- `round_trip_delay_ms_num` Set round trip delay in milliseconds. The valid range is 0–500.
- `rfactor_num` Specify R-factor number. The valid range is 0–100.
- `mos_num` Specify MOS number. The valid range is 0–5.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTCP monitoring</td>
<td>Enable</td>
</tr>
<tr>
<td>Jitter Threshold (audio/video/other)</td>
<td>50/100/100 ms</td>
</tr>
<tr>
<td>Packet-lost Threshold (audio/video/other)</td>
<td>10/20/20%</td>
</tr>
<tr>
<td>RTT Threshold (audio/video/other)</td>
<td>180/250/250 ms</td>
</tr>
<tr>
<td>R-factor Threshold (audio/video/other)</td>
<td>70/80/80</td>
</tr>
<tr>
<td>MOS Threshold (audio/video/other)</td>
<td>3.6/3.0/3.0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

Setting a threshold value to 0 disables threshold checking for that parameter.

### Examples

```
-> sip-snooping threshold audio jitter 50
```
-> sip-snooping threshold audio packet-lost 10
-> sip-snooping threshold video jitter 80
-> sip-snooping threshold video round-trip-delay 180

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

*show sip-snooping config*  
Shows the configuration done for SIP snooping.

**MIB Objects**

aluSIPSnoopingThresholdMediumIndex
  aluSIPSnoopingThresholdMedium
  aluSIPSnoopingThresholdJitter
  aluSIPSnoopingThresholdPacketLost
  aluSIPSnoopingThresholdRoundTripDelay
  aluSIPSnoopingThresholdRFactor
  aluSIPSnoopingThresholdMOS
sip-snooping logging-threshold num-of-calls

Configures the threshold for the number of calls to be logged into the flash file.

**Syntax Definitions**

*num* Specifies the maximum number of calls to be logged.

**Defaults**

By default, 200 calls can be logged.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to configure the threshold for the number of calls to be logged into the flash file.

**Examples**

```plaintext
-> sip-snooping logging-threshold num-of-calls 300
```

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

*show sip-snooping config* Displays the SIP snooping configuration for the switch.

**MIB Objects**

aluSIPSnoopingThresholdNumberOfCalls
SIP Commands

show sip-snooping call-records

show sip-snooping call-records
Displays the SIP-snooping active/ended call records.
show sip-snooping call-records {active-calls | ended-calls} [full | threshold-violation]

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:
6360

6465

6560

6570M

6860

6860N

6865

6900

6900
V72/C32

6900
X48C6/T48C6/
X48C4E/V48C8/
C32E/T24C2/
X24C2

9900

No

No

No

No

Yes

No

No

No

No

No

No

Usage Guidelines
This command is used to show the SIP-snooping active/ended call records.

Examples
-> show sip-snooping call-records ended-calls full
Legend: start date time duration media-type end-reason
call-id / from-tag / to-tag
IP address port DSCP (forward/reverse)
policy-rule (F/R)
Pkt count (F/R)
statistics min / max / avg %samples exceeding threshold (F/R)
---------------------------------------------------------------------2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal
0123456789012345678901234567890123456789012345678901234567890123 /
01234567890123456789012345678901 / 01234567890123456789012345678901
IP/DSCP 222.222.222.222 22222 63/63 111.111.111.111 11111 63/63
Policy-Rule SIP-VLAN10-Rule
SIP-VLAN10-Rule
Pkt-Count 9999999999
9999999999
Pkt-Loss
99.9 / 99.9 / 99.9 99%
99.9 / 99.9 / 99.9 99%
Jitter
999.9 / 999.9 / 999.9 99%
999.9 / 999.9 / 999.9 99%
Delay
99999 / 99999 / 99999 99%
99999 / 99999 / 99999 99%
R-factor
99.9 / 99.9 / 99.9
99.9 / 99.9 / 99.9
MOS
4.9 / 4.9
/ 4.9
4.9 / 4.9
/ 4.9

2012-01-30 09:12:30 UTC 9999d 02h 22m 03s Audio Normal

OmniSwitch AOS Release 8 CLI Reference Guide

April 2023

page 18-22


show sip-snooping call-records

Number of Call Records: 2

Number of Call Records: 1

output definitions

<table>
<thead>
<tr>
<th>Policy-Rule</th>
<th>Name of the SIP policy rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkt-Count</td>
<td>Packet Count in percentage for SIP Snooping.</td>
</tr>
<tr>
<td>Pkt-Loss</td>
<td>Packet Loss in percentage for SIP Snooping.</td>
</tr>
<tr>
<td>Jitter</td>
<td>Jitter threshold in millisecond for SIP Snooping.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay</td>
<td>Round trip delay in millisec for SIP Snooping.</td>
</tr>
<tr>
<td>R-factor</td>
<td>R-Factor for SIP Snooping.</td>
</tr>
<tr>
<td>MOS</td>
<td>MOS for SIP Snooping.</td>
</tr>
<tr>
<td>Number of Call Records</td>
<td>Number of call records that can be stored onto the device.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping config Displays the SIP snooping configuration.

MIB Objects

alaQoSDSCPEntryNumber
alaQoSDDCPPriority
alaQoSDSCPDropPrecedence
clear sip-snooping statistics

Clears all the values of SIP snooping statistics

clear sip-snooping statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is used to clear all the SIP-snooping statistics.

Examples

-> clear sip-snooping statistics

Release History

Release 8.1.1; command was introduced.

Related Commands

show sip-snooping statistics Displays SIP snooping statistics.

MIB Objects

aluSIPSnoopingClearStats
show sip-snooping config

Displays the SIP snooping configuration for the switch.

```
show sip-snooping config
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to show the SIP snooping status and configuration for the switch.

**Examples**

```
-> show sip-snooping config
Sip-snooping Status : Enable,
Sip-control DSCP     : 40,
SOS-Call RTP/RTCP DSCP : 35,
SOS-Call Numbers     : 911, 2233,
Jitter Threshold (audio/video/other) : 50ms/100ms/100ms,
Packet-Lost Threshold (audio/video/other) : 10/20/20,
Round-Trip-Delay Threshold (audio/video/other) : 180ms/250ms/250ms,
R-factor Threshold (audio/video/other) : 70/80/80,
MOS Threshold (audio/video/other) : 3.6/3.0/3.0,
Logging Number of calls : 200,
UDP-Port(s) : 5060, 5260
TCP-Port(s) : 5260
Trusted Server IP(s) : 192.254.32.11, 192.254.32.22
Reserved HW resource : 1,
CPU Rate Limiter for SIP PDUS : 1 mbps,
```

**output definitions**

- **Sip-snooping Status**: Indicates whether the SIP Snooping status is Enable or Disable.
- **Sip-control DSCP**: Displays the SIP control DSCP value.
SIP Commands

Output definitions (continued)

<table>
<thead>
<tr>
<th>Output Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOS-Call RTP/RTCP DSCP</td>
<td>Displays the SOS-Call RTP/RTCP DSCP number.</td>
</tr>
<tr>
<td>SOS-Call Number</td>
<td>Displays the emergency call number.</td>
</tr>
<tr>
<td>Jitter Threshold</td>
<td>Displays the Jitter threshold in milliseconds.</td>
</tr>
<tr>
<td>Packet-Lost Threshold</td>
<td>Displays the packet lost threshold in percentage.</td>
</tr>
<tr>
<td>Round-Trip-Delay Threshold</td>
<td>Displays the Round-Trip-Delay threshold period in milliseconds.</td>
</tr>
<tr>
<td>R-factor Threshold</td>
<td>Displays the R-Factor value.</td>
</tr>
<tr>
<td>MOS Threshold</td>
<td>Displays the MOS for SIP Snooping.</td>
</tr>
<tr>
<td>Logging Number of calls</td>
<td>Displays the maximum number of calls to be logged in flash file.</td>
</tr>
<tr>
<td>UDP-Ports</td>
<td>Displays the SIP Snooping UDP Ports.</td>
</tr>
<tr>
<td>TCP Ports</td>
<td>Displays the SIP Snooping TCP ports.</td>
</tr>
<tr>
<td>Trusted Server IP(s)</td>
<td>Displays the trusted server IP addresses.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.

Related Commands

- `show sip-snooping statistics` Displays SIP snooping statistics.
- `clear sip-snooping statistics` Clears all the logs of SIP snooping statistics

MIB Objects

aluSIPsnoopingThresholdMediumIndex
aluSIPsnoopingStatus
aluSIPsnoopingSIPControlDSCP
aluSIPsnoopingSOSCallRTPDSCP
aluSIPsnoopingSOSCallNumber1
aluSIPsnoopingSOSCallNumber2
aluSIPsnoopingSOSCallNumber3
aluSIPsnoopingSOSCallNumber4
aluSIPsnoopingThresholdMedium
aluSIPsnoopingThresholdJitter
aluSIPsnoopingThresholdPacketLost
aluSIPsnoopingThresholdRoundTripDelay
aluSIPsnoopingThresholdNumberOfCalls
aluSIPsnoopingSIPTrustedServerIPAddress1
aluSIPsnoopingSIPTrustedServerIPAddress2
aluSIPsnoopingSIPTrustedServerIPAddress3
aluSIPsnoopingSIPTrustedServerIPAddress4
aluSIPsnoopingSIPTrustedServerIPAddress5
aluSIPsnoopingSIPTrustedServerIPAddress6
aluSIPsnoopingSIPTrustedServerIPAddress7
aluSIPsnoopingSIPTrustedServerIPAddress8
aluSIPsnoopingSIPUDPPort1
aluSIPsnoopingSIPUDPPort2
aluSIPsnoopingSIPUDPPort3
aluSIPsnoopingSIPUDPPort4
aluSIPsnoopingSIPUDPPort5
aluSIPsnoopingSIPUDPPort6
<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>aluSIPSnoopingSIPUDPPort7</td>
</tr>
<tr>
<td>aluSIPSnoopingSIPUDPPort8</td>
</tr>
</tbody>
</table>
show sip-snooping ports

Displays configuration information for SIP snooping ports.

show sip-snooping ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900</td>
<td>6900</td>
<td>6900</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C6/T48C6/</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is used to show the SIP-snooping port-level data.

Examples

-> show sip-snooping ports
Legend : sip snooping : * status disabled (Sip-snooping globally disabled)
Port sip-snooping Edge/Non-edge
-----------------------------------------------
1/1 enable automatic
1/3 enable (*) force-edge
1/3 enable (*) force-non-edge

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>sip-snooping</th>
<th>Edge/Non-edge</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Displays ports configured for sip-snooping.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Displays the status of sip-snooping on the port, enable or disable.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Displays the edge status of the port.</td>
<td></td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.
**Related Commands**

*show sip-snooping statistics* Displays SIP snooping statistics.

**MIB Objects**

aluSIPSnoopingPortConfigSlotPortIndex
aluSIPSnoopingPortConfigPortStatus
aluSIPSnoopingPortConfigPortMode
show sip-snooping statistics

Displays SIP snooping statistics.

show sip-snooping statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>6900</th>
<th>X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command is used to show the SIP snooping statistics.

Examples

-> show sip-snooping statistics
Total calls processed : ,
Total audio streams : ,
Total video streams : ,
Total other streams : ,
Total audio streams that crossed threshold : ,
Total video streams that crossed threshold : ,
Total other streams that crossed threshold : ,
Active Streams that crossed threshold : ,
Number of Active calls : ,
Number of active audio streams : ,
Number of active video streams : ,
Number of active other streams : ,
Number of SIP packet received by hardware : ,
Number of SIP packet received by software : ,
Number of SIP packet received per method: INVITE(100) ACK(101) BYE(200) UPDATE(40) PRACK(20)
Number of SIP response packet received:
Number of discarded/mailed/unsupported SIP packets:
Number of discarded SIP packets not from/to trusted servers:
Number of dropped SIP packet due the software error:
(NI overflow, NI/CMM, CMM overflow)
Total Emergency Calls :
**output definitions**

<table>
<thead>
<tr>
<th>Output Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total calls processed</td>
<td>Total calls processed for SIP Snooping.</td>
</tr>
<tr>
<td>Total audio streams</td>
<td>Displays the total audio streams.</td>
</tr>
<tr>
<td>Total video streams</td>
<td>Displays the total video streams.</td>
</tr>
<tr>
<td>Total other streams</td>
<td>Displays the total other streams.</td>
</tr>
<tr>
<td>Total audio streams that crossed threshold</td>
<td>Displays the total audio streams that have exceeded threshold.</td>
</tr>
<tr>
<td>Total video streams that crossed threshold</td>
<td>Displays the total video streams that have exceeded threshold.</td>
</tr>
<tr>
<td>Total other streams that crossed threshold</td>
<td>Displays the total other streams that have exceeded threshold.</td>
</tr>
<tr>
<td>Number of Active calls</td>
<td>Displays the number of active calls.</td>
</tr>
<tr>
<td>Number of Active audio streams</td>
<td>Displays the number of active audio streams.</td>
</tr>
<tr>
<td>Number of Active video streams</td>
<td>Displays the number of active video streams.</td>
</tr>
<tr>
<td>Number of Active other streams</td>
<td>Displays the number of active other streams.</td>
</tr>
<tr>
<td>Number of SIP packet received by hardware</td>
<td>Displays the total SIP packet received by hardware.</td>
</tr>
<tr>
<td>Number of SIP packet received by software</td>
<td>Displays the total SIP packet received by software.</td>
</tr>
<tr>
<td>Number of SIP packet received by per method</td>
<td>Displays the method by which the SIP packet is received. The various per method are Invite, Ack, Bye, Update and Prack.</td>
</tr>
<tr>
<td>Number of SIP response packet received</td>
<td>Displays the total number of SIP response packet received.</td>
</tr>
<tr>
<td>Number of discarded/malformed/unsupported SIP packets</td>
<td>Displays the total number of discarded, malformed or unsupported SIP packets.</td>
</tr>
<tr>
<td>Number of discarded SIP packets not from/to trusted servers</td>
<td>Displays the total number of discarded SIP packets not from or to trusted servers</td>
</tr>
<tr>
<td>Number of dropped SIP packet due the software error</td>
<td>Displays the Total number of SIP packets dropped due the software error. (i.e. NI overflow, NI/CMM, CMM overflow etc.)</td>
</tr>
<tr>
<td>Total Emergency Calls</td>
<td>Displays the total number of Emergency Calls.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- clear sip-snooping statistics  
  Clears the SIP snooping statistics.
MIB Objects

aluSIPSnoopingTotalCallsProcessed
aluSIPSnoopingTotalAudioStreams
aluSIPSnoopingTotalVideoStreams
aluSIPSnoopingTotalOtherStreams
aluSIPSnoopingAudioStreamsBeyondThreshold
aluSIPSnoopingVideoStreamsBeyondThreshold
aluSIPSnoopingOtherStreamsBeyondThreshold
aluSIPSnoopingActiveStreamsBeyondThreshold
aluSIPSnoopingActiveAudioStreams
aluSIPSnoopingActiveVideoStreams
aluSIPSnoopingActiveOtherStreams
aluSIPSnoopingHardwareSIPPackets
aluSIPSnoopingSoftwareSIPPackets
aluSIPSnoopingSIPInvitePackets
aluSIPSnoopingSIPAckPackets
aluSIPSnoopingSIPByePackets
aluSIPSnoopingSIPByePackets
aluSIPSnoopingSIPUpdatePackets
aluSIPSnoopingSIPPrackPackets
aluSIPSnoopingSIPRecvdResponsePackets
aluSIPSnoopingSIDiscardedPackets
aluSIPSnoopingSIPDiscardedNoTrustServerPackets
aluSIPSnoopingSIPDroppedSWErrorPackets
aluSIPSnoopingTotalEmergencyCalls
show sip-snooping registered-clients

Shows the registered SIP clients learned by the switch.

show sip-snooping registered-clients

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command is used to show the registered SIP clients learned by the switch.

Examples

-> show sip-snooping registered-clients

<table>
<thead>
<tr>
<th>S/N</th>
<th>Registered Client IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.135.22.18</td>
</tr>
<tr>
<td>2</td>
<td>10.135.22.25</td>
</tr>
<tr>
<td>3</td>
<td>10.135.23.124</td>
</tr>
</tbody>
</table>

Output definitions

<table>
<thead>
<tr>
<th>Registered Client IP Address</th>
<th>The IP address of the registered client.</th>
</tr>
</thead>
</table>

Release History
Release 8.1.1; command was introduced.
Related Commands

**sip-snooping port admin-state**  
Configures the status of SIP snooping on a single port, a range of ports, or on a link aggregate.

MIB Objects

- a1aSIPSnoopingRegisteredClientNumber
- a1aSIPSnoopingRegisteredClientAddrType
- a1aSIPSnoopingRegisteredClientAddr
19 Automatic Fabric Commands

The Dynamic Auto-Fabric feature can be used to bring up AOS compatible devices by automating some tedious and complex steps including Link Aggregate formation, and SPB neighbor adjacency formation. Dynamic recognition of the neighboring elements will allow a quick, out-of-the box configuration. The focus area for this feature is data center but the feature is applicable in campus LAN environment to reduce administrative overhead.

Upon boot-up the system will automatically attempt auto discovery of LACP, SPB, MVRP, and IP connections if configuration files are not available in the device. The feature allows to build a true fabric when a device is plugged to the network and automates edge port configuration with profiles.

MIB information for the Auto Fabric commands is as follows:

- Filename: ALCATEL-IND1-AUTO-FABRIC-MIB.mib
- Module: alcatelIND1AUTOFABRICMIB

A summary of available commands is listed here:

```
auto-fabric admin-state
auto-fabric interface
auto-fabric discovery start
auto-fabric protocols
auto-fabric config-save interval
auto-fabric config-save admin-state
auto-fabric discovery-interval
auto-fabric protocols spb default-profile
auto-fabric protocols spb set-profile
show auto-fabric config
show auto-fabric config interface
```
**auto-fabric admin-state**

Enables or disables the Automatic Fabric functionality globally for the switch.

```bash
auto-fabric admin-state {enable | disable {remove-global-config | remove-vc-reload}}
```

### Syntax Definitions

- **enable**
  Enables Automatic Fabric functionality for the switch.

- **disable**
  Enables Automatic Fabric functionality for the switch. When disabled, the global configuration settings discovered for MVRP, SPB, and IP are removed.

- **remove-global-config**
  Disables Automatic Fabric functionality for the switch. This parameter option performs the same function as the **disable** parameter.

- **remove-vc-reload**
  Reboots a switch running in the Virtual Chassis (VC) of one mode to run in the standalone mode with Automatic Fabric discovery disabled. This parameter option is not supported on the OmniSwitch 6860 and OmniSwitch 6865.

### Defaults

By default, the Automatic Fabric operation is globally enabled for the switch and on all eligible interfaces when the switch boots up without a configuration file (such as boot.cfg) or the configuration file size is zero bytes.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When a switch boots up with an existing configuration file, the Automatic Fabric operation is based on the administrative status setting specified with this command.

- When Automatic Fabric is globally disabled for the switch, the following configuration settings are removed unless they were previously saved to the switch configuration file:
  - Spanning Tree is set back to the default 1x1 mode. This only occurs if there are no VLAN registrations on any port or link aggregate.
  - SPB is globally disabled, which removes BVLANs 4000-4003 and administratively disables SPB. This only occurs if there are no SPB adjacencies formed on any ports or link aggregates.
  - Automatic Fabric stops trying to learn IP routing protocols and neighbors on interfaces not already configured with a routing protocol. The configuration for IP interfaces on which routing protocols
were previously discovered is not removed.
  – For any other scenario, administrator intervention is needed to remove the configuration.

- The **remove-global-config** and **remove-vc-config** parameters are only used in combination with the **disable** option.

- The **remove-vc-config** parameter is only meant for use when a switch has booted up in a VC of one mode. Do not use this option if the switch boots up as part of a VC configuration, where the switch is connected to other switches in the VC.

- When this command is used with the **remove-vc-config** parameter, the following process is triggered:
  1. Any Automatic Fabric configuration is cleared.
  2. The Automatic Fabric feature is disabled.
  3. A **boot.cfg** file is created in the /flash/working directory.
  4. The switch is automatically rebooted in standalone mode with a configuration file and the automatic management features will no longer run.

**Examples**

- `-> auto-fabric admin-state enable`
- `-> auto-fabric admin-state disable`
- `-> auto-fabric admin-state disable remove-global-config`
- `-> auto-fabric admin-state disable remove-vc-reload`

**Release History**

Release 7.3.2; command introduced.
Release 7.3.4; **remove-global-config** and **remove-vc-reload** parameters added-

**Related Commands**

- **auto-fabric interface** Enables or disables Automatic Fabric discovery on one or more ports.
- **show auto-fabric config interface** Displays the Automatic Fabric configuration applied to switch ports.

**MIB Objects**

- alaAutoFabricGlobalStatus
- alaAutoFabricRemoveGlobalConfig
- alaAutoFabricRemoveVCReload
**auto-fabric interface**

Enables or disables the Automatic Fabric functionality for one or more switch ports.

```
auto-fabric interface chassis/slot/port[-port2] admin-state {enable | disable}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **enable**: Enables Automatic Fabric functionality globally or on an interface.
- **disable**: Disables Automatic Fabric functionality on the specified interface. When disabled, the configuration settings discovered for MVRP, SPB, and IP are removed from the port.

### Defaults

By default, the Automatic Fabric operation is globally enabled for the switch and on all eligible interfaces when the switch boots up without a configuration file (such as boot.cfg) or the configuration file size is zero bytes.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When a switch boots up with an existing configuration file, the Automatic Fabric status for a port is based on the administrative status setting specified with this command.

- The Automatic Fabric status for a specific port takes precedence over the global Automatic Fabric status for the switch. For example, if Automatic Fabric is enabled for the switch but disabled on a port, then the discovery process is not run on the port.

### Examples

```
-> auto-fabric interface 1/1/1 admin-state disable
-> auto-fabric interface 1/1/5-10 admin-state enable
```

### Release History

Release 7.3.2; command introduced.
**Related Commands**

- **auto-fabric admin-state**
  Globally enables or disables Automatic Fabric for the switch.

- **show auto-fabric config interface**
  Displays the Automatic Fabric configuration applied to switch ports.

**MIB Objects**

- **alaAutoFabricPortConfigTable**
- **alaAutoFabricPortConfigStatus**
**auto-fabric discovery start**

Manually starts the Automatic Fabric discovery process.

```plaintext
auto-fabric discovery start
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command can be used to manually begin the Automatic Fabric discovery process after the switch has booted and the discovery window has elapsed.

### Examples

```plaintext
-> auto-fabric discovery start
```

### Release History

Release 7.3.2; command introduced.

### Related Commands

- `show auto-fabric config` Displays the global Automatic Fabric configuration.
- `show auto-fabric config interface` Displays Automatic Fabric configuration applied on interfaces.

### MIB Objects

- `alaAutoFabricGlobalDiscovery`
**auto-fabric protocols**

Enables or disables the Automatic Fabric discovery process for a particular protocol.

```
auto-fabric protocols {lacp | mvrp | spb | ip {ospfv2 | ospfv3 | isis | all} | loopback-detection}
{interface chassis/slot/port-port2 | chassis} admin-state {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lacp</td>
<td>Selects the Link Aggregation Control Protocol.</td>
</tr>
<tr>
<td>mvrp</td>
<td>Selects the Multiple VLAN Registration Protocol.</td>
</tr>
<tr>
<td>spb</td>
<td>Selects the Shortest Path Bridging protocol. This parameter option is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.</td>
</tr>
<tr>
<td>ospfv2</td>
<td>Selects the Open Shortest Path First version 2 protocol. This parameter option is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.</td>
</tr>
<tr>
<td>ospfv3</td>
<td>Selects the Open Shortest Path First version 3 protocol. This parameter option is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.</td>
</tr>
<tr>
<td>isis</td>
<td>Selects the Intermediate System-Intermediate System protocol. This parameter option is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M or OmniSwitch 9900.</td>
</tr>
<tr>
<td>all</td>
<td>Selects all the supported IP routing protocols (OSPFv2, OSPFv3, and IS-IS).</td>
</tr>
<tr>
<td>loopback-detection</td>
<td>Selects Loopback Detection for UNP SPB access ports. Access ports are used to create SPB Service Access Points (SAP).</td>
</tr>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port[-port2]</td>
<td>The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).</td>
</tr>
<tr>
<td>chassis</td>
<td>All Automatic Fabric ports on the chassis. Use this parameter to globally configure the discovery status for the selected protocol.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the discovery status for the selected protocol.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the discovery status for the selected protocol.</td>
</tr>
</tbody>
</table>

### Defaults

- Automatic Fabric discovery is globally enabled for all the protocols when the switch boots up without a configuration file.
- Automatic Fabric discovery is globally enabled for all protocols, except MVRP, when the switch boots up with an existing configuration file. In this case, the global default setting for MVRP is disabled.
- Automatic Fabric discovery is enabled for LACP, MVRP, and SPB on all eligible interfaces by default.
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If no interface is specified with this command, the discovery status for the protocol is enabled or disabled globally for the switch.

- The `interface` and `chassis` parameters are only used in combination with the `lacp`, `mvrp`, and `spb` parameters.

- The interface setting for LACP, MVRP, and SPB discovery overrides the global setting. For example, if SPB discovery is globally enabled for the switch but disabled on port 2/1/1, then the port does not participate in the SPB discovery process.

Examples

- `auto-fabric protocols lacp admin-state disable`
- `auto-fabric protocols mvrp admin-state enable`
- `auto-fabric protocols spb interface 1/1/3 admin-state disable`
- `auto-fabric protocols loopback-detection admin-state disable`
- `auto-fabric protocols ip ospfv2 admin-state enable`
- `auto-fabric protocols ip ospfv3 admin-state disable`
- `auto-fabric protocols ip isis admin-state disable`

Release History

Release 7.3.2; command introduced.
Release 7.3.4; `loopback-detection` and `ip` parameters added.
Release 8.3.1; default setting for global MVRP discovery is disabled when switch boots up with an existing configuration file.

Related Commands

- `auto-fabric admin-state`: Enables or disables Automatic Fabric functionality.
- `show auto-fabric config interface`: Displays the Automatic Fabric configuration applied on interfaces.
- `show auto-fabric config`: Displays the global Automatic Fabric configuration.
MIB Objects

alaAutoFabricGlobalLACPProtocolStatus
alaAutoFabricGlobalSPBProtocolStatus
alaAutoFabricGlobalMVRPProtocolStatus
alaAutoFabricGlobalOSPFv2Status
alaAutoFabricGlobalOSPFv3Status
alaAutoFabricGlobalISISStatus
alaAutoFabricLBDProtocolStatus

alaAutoFabricPortConfigTable
alaAutoFabricPortLACPProtocolStatus
alaAutoFabricPortSPBProtocolStatus
alaAutoFabricPortMVRPProtocolStatus
**auto-fabric config-save interval**

Configures the time interval for saving the automatically discovered configuration to the switch configuration file.

**auto-fabric config-save interval** *seconds*

---

**Syntax Definitions**

- **seconds**
  
  The amount of time between automatic saves of the discovered configuration. Range is 60 - 3600 seconds.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>300</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The automatic save time interval specified with this command is only valid when the automatic configuration save status is enabled. This is done through the **auto-fabric config-save admin-state** command.

---

**Examples**

```
-> auto-fabric config-save interval 600
```

---

**Release History**

Release 7.3.2; command introduced.
Related Commands

- **auto-fabric config-save admin-state**
  Enables or disables automatically saving of the discovered configuration to the switch configuration file.

- **show auto-fabric config**
  Displays the Automatic Fabric configuration.

MIB Objects

- **alaAutoFabricGlobalConfigSaveTimer**
**auto-fabric config-save admin-state**

Enables or disables automatically saving of the discovered configuration to the switch configuration file.

```
auto-fabric config-save admin-state {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables automatically saving the discovered configuration to the switch configuration file.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables automatically saving the discovered configuration to the switch configuration file.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, automatically saving the discovered configuration is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When this function is enabled, the amount of time specified through the `auto-fabric config-save interval` command is active. An automatic save is performed whenever the specified amount of time elapses.

**Examples**

```
-> auto-fabric config-save admin-state disable
```

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- **auto-fabric config-save interval** Configures the amount of time to wait between automatic saves of the discovered configuration.
- **show auto-fabric config** Displays the Automatic Fabric configuration.

**MIB Objects**

- `alaAutoFabricGlobalConfigSaveTimerStatus`
auto-fabric discovery-interval

Configures when the switch will automatically start the Automatic Fabric discovery process.

**auto-fabric discovery-interval minutes**

### Syntax Definitions

**minutes** The discovery interval time. The valid range is 2–3600 minutes.

### Defaults

By default, the discovery interval timer is set to zero (disabled).

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When a switch boots up without a configuration file, discovery is automatically started for a one-time, initial run even when the interval timer is disabled.

- Set the value of this timer to more than two times the value of the switch MAC address aging time. This will allow time for inactive MAC addresses to age out on Automatic Fabric ports before the next discovery interval is started.

### Examples

`-> auto-fabric discovery-interval 60`

### Release History

- Release 7.3.2; command introduced.
- Release 7.3.4; timer default value changed to zero (disabled).

### Related Commands

- **show auto-fabric config** Displays the Automatic Fabric configuration.

### MIB Objects

- *alaAutoFabricGlobalDiscoveryTimer*
**auto-fabric protocols spb default-profile**

Configures the default Service Access Point (SAP) profile that the Universal Network Profile (UNP) feature uses to dynamically create SAPs for traffic received on UNP access ports.

```
auto-fabric protocols spb default-profile {single-service | auto-vlan}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>single-service</td>
<td>Dynamically creates a SAP profile only for untagged traffic on the UNP access port.</td>
</tr>
<tr>
<td>auto-vlan</td>
<td>Dynamically creates a SAP for each VLAN tag received on a UNP access port. When this option is selected, the <code>single-service</code> option is automatically triggered for untagged traffic.</td>
</tr>
</tbody>
</table>

### Defaults

By default, the switch is set to use the `auto-vlan` option.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- A SAP is a logical service entity (also referred to as a virtual port) that binds an access port to an SPB service ID and specifies the type of customer traffic (untagged or tagged) to encapsulate and tunnel through the SPB network infrastructure.
- Once the SPB adjacencies and UNP access ports are configured through Automatic Fabric discovery, traffic received on UNP access ports triggers the switch to dynamically create a SAP for the traffic based on the SAP profile selected with this command.

### Examples

```
-> auto-fabric protocols spb default-profile single-service
-> auto-fabric protocols spb default-profile auto-vlan
```

### Release History

Release 7.3.4; command introduced.
Related Commands

**auto-fabric protocols spb set-profile**
Configures the default SAP profile for a specific port or range of ports on the switch.

**show auto-fabric config**
Displays the global Automatic Fabric configuration.

**show auto-fabric config interface**
Displays Automatic Fabric configuration applied on interfaces.

MIB Objects

alaAutoFabricSPBDefaultProfile
**auto-fabric protocols spb set-profile**

Configures the default SAP profile for a specific port or range of ports on the switch.

```
auto-fabric protocols spb set-profile {single-service | auto-vlan} interface chassis/slot/port[-port2]
```

### Syntax Definitions

- **single-service**
  
  Defines single default service SAP profile. Only untagged traffic on the UNP port is learned in this profile.

- **auto-vlan**
  
  The incoming traffic is automatically learned. The SAP bindings for the concerned VLANs are automatically created based on the traffic sensed.

- **chassis**
  
  The chassis identifier.

- **slot/port[-port2]**
  
  The slot and port number (3/1) on which the SAP profile will be enabled. Use a hyphen to specify a range of ports (3/1-8).

### Defaults

By default, the **auto-vlan** option is used for Automatic Fabric ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The SAP profile configured for the specified port or range of ports overrides the default SAP profile configured for the switch.

### Examples

```
-> auto-fabric protocols spb set-profile single-service interface 1/1/1
-> auto-fabric protocols spb set-profile auto-vlan interface 1/2/1-4
```

### Release History

Release 7.3.4; command introduced.
**Related Commands**

- `show auto-fabric config` Displays the auto-fabric configuration.
- `show auto-fabric config interface` Displays auto-fabric configuration applied on interfaces.

**MIB Objects**

- `alaAutoFabricPortConfigTable`
- `alaAutoFabricPortConfigIfIndex`
- `alaAutoFabricPortSPBDefaultProfile`
show auto-fabric config

Displays the Automatic Fabric configuration.

show auto-fabric config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show auto-fabric config
Auto-fabric Status : Disable,
Config Save Timer Status : Disabled,
Config Save Timer Interval : 300 seconds,
Default UNP SAP Profile : Auto-vlan,
Discovery Interval : 1 minute(s),
Discovery Status : Idle,
LACP Discovery Status : Enabled,
LBD Discovery Status : Enabled,
MVRP Discovery Status : Disabled,
OSPFv2 Discovery Status : Enabled,
OSPFv3 Discovery Status : Enabled,
ISIS Discovery Status : Enabled,
SPB Discovery Status : Enabled

output definitions

<table>
<thead>
<tr>
<th>Auto-Fabric Status</th>
<th>Config Save Timer Status</th>
<th>Config Save Timer Interval</th>
<th>Default UNP SAP Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>The global status of the Automatic Fabric functionality.</td>
<td>The status of the Automatic Fabric configuration save timer.</td>
<td>How often the discovered Automatic Fabric configuration is saved to the switch configuration file.</td>
<td>The default SAP profile for the switch.</td>
</tr>
</tbody>
</table>
Automatic Fabric Commands

show auto-fabric config

output definitions (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery Interval</td>
<td>How often the Automatic Fabric discovery process will run.</td>
</tr>
<tr>
<td>Discovery Status</td>
<td>Whether the global discovery process is running or idle.</td>
</tr>
<tr>
<td>LACP Discovery Status</td>
<td>The global status of Automatic Fabric discovery for the LACP protocol.</td>
</tr>
<tr>
<td>LBD Discovery Status</td>
<td>The status of the Loopback Detection on dynamically created UNP Service Access Points (SAPs).</td>
</tr>
<tr>
<td>MVRP Discovery Status</td>
<td>The global status of Automatic Fabric discovery for the MVRP protocol.</td>
</tr>
<tr>
<td>OSPFv2 Discovery Status</td>
<td>The global status of Automatic Fabric discovery for the OSPFv2 protocol.</td>
</tr>
<tr>
<td>OSPFv3 Discovery Status</td>
<td>The global status of Automatic Fabric discovery for the OSPFv3 protocol.</td>
</tr>
<tr>
<td>ISIS Discovery Status</td>
<td>The global status of Automatic Fabric discovery for the ISIS protocol.</td>
</tr>
<tr>
<td>SPB Discovery Status</td>
<td>The global status of Automatic Fabric discovery for the SPB protocol.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command introduced.
Release 7.3.4; OSPFv2 Discovery Status, OSPFv3 Discovery status, ISIS Discovery Status, LBD Discovery Status, and Default UNP SAP Profile output fields added.

Related Commands

- **auto-fabric admin-state**: Enables or disables Automatic Fabric functionality.
- **auto-fabric config-save admin-state**: Configures the status of the Automatic Fabric configuration save timer.
- **auto-fabric config-save interval**: Configures how often the discovered Automatic Fabric configuration is saved to the switch configuration file.
- **auto-fabric protocols spb default-profile**: Configures the default SAP profile for the switch.
- **auto-fabric discovery-interval**: Configures how often the Automatic Fabric discovery process will run.
- **auto-fabric protocols**: Enables or disables Automatic Fabric discovery for specific protocols.

MIB Objects

AutoFabTable
  - alaAutoFabricGlobalStatus
  - alaAutoFabricGlobalDiscovery
  - alaAutoFabricGlobalLACPProtocolStatus
  - alaAutoFabricGlobalSPBProtocolStatus
  - alaAutoFabricGlobalMVRPProtocolStatus
  - alaAutoFabricGlobalConfigSaveTimer
  - alaAutoFabricGlobalConfigSaveTimerStatus
  - alaAutoFabricGlobalDiscoveryTimer
  - alaAutoFabricGlobalOSPFv2ProtocolStatus
  - alaAutoFabricGlobalOSPFv3ProtocolStatus
  - alaAutoFabricGlobalISISProtocolStatus
  - alaAutoFabricSPBDefaultProfile
show auto-fabric config

alaAutoFabricLBDProtocolStatus
show auto-fabric config interface

Displays the Automatic Fabric configuration applied on interfaces.

`show auto-fabric config interface [chassis/slot[-slot2] | chassis/slot/port[-port2]]`

**Syntax Definitions**

- **chassis**
  The chassis identifier.

- **slot[-slot2]**
  The slot number. Use a hyphen to specify a range of slot numbers (1/1-5 displays ports on slots 1 through 5).

- **slot/port[-port2]**
  The chassis ID, slot, and port number. Use a hyphen to specify a range of ports (1/1/2-10 displays ports 1 through 10).

**Defaults**

By default, the Automatic Fabric configuration for all switch ports is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>Supported Platforms</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To display the global and port-level configuration for specific interfaces, specify a port number with this command.

**Examples**

```
->show auto-fabric config interface
```

```
<table>
<thead>
<tr>
<th>Port</th>
<th>Admin Status</th>
<th>LACP</th>
<th>SPB-M</th>
<th>MVRP</th>
<th>SAP Profile</th>
<th>Oper Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>disabled</td>
<td>enabled</td>
<td>enabled</td>
<td>disabled</td>
<td>single-service</td>
<td>disabled</td>
</tr>
<tr>
<td>1/1/2</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled</td>
<td>disabled</td>
<td>auto-vlan</td>
<td>disabled</td>
</tr>
<tr>
<td>1/1/3</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled</td>
<td>auto-vlan</td>
<td>disabled</td>
</tr>
<tr>
<td>1/1/4</td>
<td>enabled</td>
<td>enabled</td>
<td>disabled</td>
<td>enabled</td>
<td>auto-vlan</td>
<td>disabled</td>
</tr>
<tr>
<td>1/1/5</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled</td>
<td>auto-vlan</td>
<td>disabled</td>
</tr>
<tr>
<td>1/1/6</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled</td>
<td>auto-vlan</td>
<td>disabled</td>
</tr>
</tbody>
</table>

**output definitions**

- **Port**
  The chassis ID, slot, and port number.

- **Admin-Status**
  The Automatic Fabric administrative status for the port.
output definitions (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACP</td>
<td>The LACP discovery status for the port.</td>
</tr>
<tr>
<td>SPB-M</td>
<td>The SPB-M discovery status for the port.</td>
</tr>
<tr>
<td>MVRP</td>
<td>The MVRP discovery status for the port.</td>
</tr>
<tr>
<td>SAP Profile</td>
<td>The default SAP profile assigned to the port.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The Automatic Fabric operational status for the port.</td>
</tr>
</tbody>
</table>

```
-> show auto-fabric config interface 1/1/1
Auto-Fabric Interface Config:
  Port 1/1/1:
    Operational Status : Disabled
    Admin-Status
      Global : Disabled,   Port : Disabled
    LACP
      Global : Enabled,    Port : Enabled
    SPB-M
      Global : Enabled,    Port : Enabled
    MVRP
      Global : Enabled,    Port : Disabled
    SAP Profile
      Global : Auto-vlan,   Port : Single-service
```

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The chassis ID, slot, and port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operational Status</td>
<td>The Automatic Fabric operational status.</td>
</tr>
<tr>
<td>Admin-Status</td>
<td>The global and port-level administrative status for Automatic Fabric.</td>
</tr>
<tr>
<td>LACP</td>
<td>The global and port-level discovery status for LACP.</td>
</tr>
<tr>
<td>SPB-M</td>
<td>The global and port-level discovery status for SPB-M.</td>
</tr>
<tr>
<td>MVRP</td>
<td>The global and port-level discovery status for MVRP.</td>
</tr>
<tr>
<td>SAP Profile</td>
<td>The global SAP profile and port-level SAP profile.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command introduced.
Release 7.3.4; SAP Profile and Operational status output fields added.

Related Commands

- **auto-fabric admin-state**: Enables or disables Automatic Fabric functionality.
- **auto-fabric protocols**: Enables or disables the Automatic Fabric discovery process for a particular protocol.
- **auto-fabric protocols spb default-profile**: Configures the default SAP profile for the switch.
- **auto-fabric protocols spb set-profile**: Configures the default SAP profile for a specific port or range of ports.
MIB Objects

alaAutoFabricGlobalStatus
alaAutoFabricGlobalLACPProtocolStatus
alaAutoFabricGlobalSPBProtocolStatus
alaAutoFabricGlobalMVRPProtocolStatus
alaAutoFabricPortConfigTable
   alaAutoFabricPortConfigIfIndex
   alaAutoFabricPortConfigStatus
alaAutoFabricPortLACPProtocolStatus
alaAutoFabricPortSPBProtocolStatus
alaAutoFabricPortMVRPProtocolStatus
alaAutoFabricPortStatus
alaAutoFabricPortSPBDefaultProfile
20   IP Commands

This chapter details Internet Protocol (IP) commands for the switch. IP is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be forwarded. IP is documented in RFC 791 and is the primary network-layer protocol in the Internet protocol suite. Along with the Transmission Control Protocol (TCP), IP represents the heart of the Internet protocols.

IP is enabled on the switch by default and there are few options that can, or need to be, configured. This chapter provides instructions for basic IP configuration commands. It also includes commands for several Layer 3 and Layer 4 protocols that are associated with IP:

- **Address Resolution Protocol (ARP)—** Used to match the IP address of a device with its physical (MAC) address.

- **Internet Control Message Protocol (ICMP)—** Specifies the generation of error messages, test packets, and informational messages related to IP. ICMP supports the **ping** command that is used to determine if hosts are online.

- **Transmission Control Protocol (TCP)—** A major data transport mechanism that provides reliable, connection-oriented, full-duplex data streams. While the role of TCP is to add reliability to IP, TCP relies upon IP to do the actual delivering of datagrams.

- **User Datagram Protocol (UDP)—** A secondary transport-layer protocol that uses IP for delivery. UDP is not connection-oriented and does not provide reliable end-to-end delivery of datagrams. But some applications can safely use UDP to send datagrams that do not require the extra overhead added by TCP.

The IP commands also include protection from Denial of Service (DoS) attacks. The goal of this feature is to protect a switch from well-known DoS attacks and to notify the administrator or manager when an attack is underway. Also, notifications can be sent when port scans are being performed.

**Note.** If all devices are on the same VLAN or if the IP interfaces are created on multiple VLANs to enable routing of packets, packets can be forwarded using IP. However, IP routing requires one of the IP routing protocols: Routing Information Protocol (RIP) or Open Shortest Path First (OSPF). See the following chapters for the appropriate CLI commands: Chapter 20, “IP Commands,” Chapter 27, “OSPF Commands.” For more information on VLANs and RIP, see the applicable chapters in the Configuration Guide. For more information on OSPF, see the “Configuring OSPF” chapter in the *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide.*
MIB information for the IP commands is as follows:

- **Filename:** IP-FORWARD-MIB.mib
  - **Module:** ipForward

- **Filename:** IP-MIB.mib
  - **Module:** ipMIB

- **Filename:** ALCATEL-IND1-IP-MIB.mib
  - **Module:** alcatelIND1IPMIB

- **Filename:** ALCATEL-IND1-IPRM-MIB.mib
  - **Module:** alcatelIND1IPRMMIB

A summary of the available commands is listed here:

```
IP
  ip interface
  ip interface rtr-port
  ip interface tunnel
  ip interface dhcp-client
  ip router primary-address
  ip router router-id
  ip static-route
  ip static-route all bfd-state
  ip static-route bfd-state
  ip route-pref
  ip default-ttl
  ping
  traceroute
  ip directed-broadcast
  ip directed-broadcast trusted-source-ip
  ip directed-broadcast clear
  show ip directed-broadcast
  ip service
  ip service port
  ip service source-ip
  ip tep time-stamp-response
  show ip interface
  show ip emp-interfaces
  show ip routes
  show ip route-pref
  show ip redist
  show ip redist-routes
  show ip access-list
  show ip route-map
  show ip router database
  show ip emp-routes
  show ip config
  show ip protocols
  show ip router-id
  show ip service
  show ip service source-ip
```
## IP Route Map Redistribution
- **ip redist**
- **ip access-list**
- **ip access-list address**
- **ip route-map action**
- **ip route-map match ip address**
- **ip route-map match ipv6 address**
- **ip route-map match ip-nexthop**
- **ip route-map match ipv6-nexthop**
- **ip route-map match tag**
- **ip route-map match ipv4-interface**
- **ip route-map match ipv6-interface**
- **ip route-map match metric**
- **ip route-map match route-type**
- **ip route-map match protocol**
- **ip route-map match name**
- **ip route-map set metric**
- **ip route-map set metric-type**
- **ip route-map set tag**
- **ip route-map set community**
- **ip route-map set local-preference**
- **ip route-map set level**
- **ip route-map set ip-nexthop**
- **ip route-map set ipv6-nexthop**
- **show ip redist**
- **show ip redist-routes**
- **show ip access-list**
- **show ip route-map**

## Multiple Virtual Routing and Forwarding (VRF)
- **vrf**
- **show vrf**
- **show vrf-profiles**

## Route Leak
- **ip export**
- **ip import**
- **show ip export**
- **show ip import**
- **show ip global-route-table**

## ARP
- **arp**
- **ip distributed-arp admin-state**
- **arp send-gratuitous-arp**
- **ip dos arp-poison restricted-address**
- **arp filter**
- **arp send-gratuitous-arp**
- **clear arp filter**
- **show arp**
- **show ip dos arp-poison**
- **show ip arp utilization**
- **show arp filter**
- **show arp send-gratuitous-arp**

## ICMP
- **icmp type**
- **icmp unreachable**
- **icmp echo**
- **icmp timestamp**
- **icmp addr-mask**
- **icmp messages**
- **show arp send-gratuitous-arp**
- **show icmp statistics**
## IP Commands

### TCP
- `ip tcp half-open-timeout`
- `ip tcp time-stamp-response`
- `show tcp statistics`
- `show tcp ports`
- `show ip tcp half-open-timeout`
- `show ip tcp time-stamp-response`

### UDP
- `show udp statistics`
- `show udp ports`

### Denial of Service (DoS)
- `ip dos scan close-port-penalty`
- `ip dos scan tcp open-port-penalty`
- `ip dos scan udp open-port-penalty`
- `ip dos scan threshold`
- `ip dos trap`
- `ip dos scan decay`
- `ip dos type`
- `show ip dos config`
- `show ip dos statistics`
**ip interface**

Configures an IP interface to enable IP routing on a VLAN or allow remote access. Without an IP interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

```
ip interface {if_name | emp | master emp | local chassis-id chassis} [{address | vip-address} ip_address] [mask subnet_mask] [admin-state [enable | disable]] [vlan vlan_id | service service_id] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [e2 | snap] [primary | no primary]
no ip interface if_name
```

### Syntax Definitions

- **if_name**
  - Text string of the interface name. Use quotes around string if description contains multiple words with spaces between them (for example, “ALE Marketing”). This value is case sensitive.

- **emp**
  - Modifies the shared EMP port IP address.

- **master emp**
  - Modifies the EMP port IP address of the master chassis when operating in virtual chassis mode.

- **local chassis-id chassis**
  - Modifies the EMP port IP address of the local chassis.

- **address ip_address**
  - An IP host address (for example, 10.0.0.1, 171.15.0.20) to specify the IP router network.

- **vip-address ip_address**
  - An IP host address for a Virtual IP (VIP) VLAN.

- **subnet_mask**
  - A valid IP address mask (for example, 255.0.0.0, 255.255.0.0) to identify the IP subnet for the interface.

- **enable**
  - Enables the administrative status for the IP interface.

- **disable**
  - Disables the administrative status for the IP interface.

- **vlan_id**
  - An existing VLAN ID number (1–4094).

- **service_id**
  - An existing Shortest Path Bridging (SPB) or L2 GRE tunneling service ID number (1–32767). This parameter is supported only on the OmniSwitch 6860N, OmniSwitch 6900-X48C6/T48C6, OmniSwitch 6900-X48C4E, and OmniSwitch 9900.

- **forward**
  - Enables forwarding of IP frames to other subnets.

- **no forward**
  - Disables forwarding of IP frames. The router interface still receives frames from other hosts on the same subnet.

- **local-proxy-arp**
  - Enables Local Proxy ARP on the specified interface.

- **no local-proxy-arp**
  - Disables Local Proxy ARP on the specified interface.

- **e2**
  - Enter e2 or ethernet2 to specify Ethernet-II encapsulation.

- **snap**
  - SNAP encapsulation.

- **primary**
  - Designates the specified IP interface as the primary interface for the VLAN.

- **no primary**
  - Removes the configured primary IP interface designation for the VLAN. The first interface bound to the VLAN becomes the primary by default.
Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>IP address class</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>vlan_id</td>
<td>service_id</td>
</tr>
<tr>
<td>forward</td>
<td>no forward</td>
</tr>
<tr>
<td>local-proxy-arp</td>
<td>no local-proxy-arp</td>
</tr>
<tr>
<td>e2</td>
<td>snap</td>
</tr>
<tr>
<td>primary</td>
<td>no primary</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove an IP interface.
- IP multinetting is supported on VLANs. As a result, it is possible to configure up to 16 IP interfaces per VLAN. Each interface is configured with a different subnet, thus allowing traffic from each configured subnet to coexist on the same VLAN.
- When local proxy ARP is enabled for any one IP router interface associated with a VLAN, the feature is applied to the entire VLAN. It is not necessary to enable it for each interface. However, if the IP interface that has this feature enabled is moved to another VLAN, Local Proxy ARP is enabled for the new VLAN and must be enabled on another interface for the old VLAN.
- When Local Proxy ARP is enabled, all traffic is routed instead of bridged within the VLAN. ARP requests return the MAC address of the IP router interface. The same MAC address is assigned to each interface configured for a VLAN.
- Local Proxy ARP takes precedence over any switch-wide ARP or Proxy ARP function. It is not necessary to have Proxy ARP configured to use Local Proxy ARP. The two features are independent of each other.
- By default, the first interface bound to a VLAN becomes the primary interface for that VLAN. Use the primary keyword with this command to configure a different IP interface as the primary. Note that this option is not supported with interfaces bound to an SPB service, as multinetting is not supported on a service. There is only one IP interface per service allowed.
To create an IP interface for network management purposes, specify **Loopback0** (case sensitive) as the name of the interface. The Loopback0 interface is not bound to any VLAN, so it always remains operationally active.

Specify the **service** parameter to create a service-based interface that is used to provide in-line routing for SPB and L2 GRE tunneling services. When creating an IP interface for an SPB service or an L2 GRE tunneling service, consider the following:

- The service ID specified must already exist in the switch configuration.
- VLAN translation is automatically enabled when a service is assigned to an IP interface regardless of whether or not VLAN translation is enabled for the service; the VLAN translation status is no longer configurable as long as the service is bound to an IP interface.
- When the last IP interface is removed from a service, the VLAN translation status will return to its previous state. For example, if the administrative status was previously disabled, the status will revert to a disabled state when there are no more IP interfaces assigned to that service.
- Mixing switches with VLAN translation enabled on some and disabled on other switches in the same network is not recommended. Make sure all switches have VLAN translation enabled, especially if a switch with a service-based interface is added to the network.
- The same SPB service ID can be assigned to an IPv4 and an IPv6 interface as long as both interface types are in the same VRF instance.
- See the “IP over SPBM” section in the “Configuring Shortest Path Bridging” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide for more information.

Configure an IP interface on an SPB control BVLAN to support in-band management access in the SPBM domain. When creating an IP interface on a control BVLAN, consider the following:

- The IP interface must be configured only on the Control BVLAN. Only IPv4 interface is supported.
- Only one Control BVLAN can be configured on a switch. This IP interface is considered operationally active when the underlying Control BVLAN becomes operationally up and all underlying configuration is considered valid.
- Whenever the IP interface is operationally down due to an unsupported configuration, the **show ip interface** command will display "Operational State Reason" as "invalid-config".
- ISIS-SPB is the only protocol supported in the IP BVLAN domain for exchanging or advertising IP routing information. No other routing protocol (including VRRP) is supported.
- Multi-netting of IP interfaces on a BVLAN is not supported. Only one IP interface must be configured on the Control BVLAN.
- STP is not allowed on BVLANs, and all broadcast packets will be restricted on this IP interface. Hence, explicit ARP/ND resolution is not supported. ISIS-SPB will provide the MAC-to-IP address mappings, to avoid broadcast packets in the SPBM backbone domain.
- The ARPs learned with ISIS-SPB on the Control BVLAN will be shown as static ARPs, but these ARPs will have bit "M" (Managed ARP) set in the ARP flags, and displayed as “M” in the “Flags” field of the **show arp** command display.
- Static routes can be configured to route packets to destinations outside of the IP BVLAN subnet or management network routes can be redistributed into ISIS-SPB at one or more SPB Backbone Edge Bridges (BEBs) that connect to a management station. ISIS-SPB then advertises the management network routes, along with the locally configured IP Looback0 address and IP BVLAN address, to all SPB nodes in the network.
- Dynamic routing protocols are not supported on this IP interface.
- The IP BVLAN domain will operate in IP unicast mode, hence IP Multicast is not supported.
- SPB in-band management is not supported on the OmniSwitch 6360, OmniSwitch 6465,
OmniSwitch 6560 and OmniSwitch 6570M.
  – See the “Configuring Shortest Path Bridging” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide for more information.

Examples

-> ip interface Marketing
-> vrf 100 ip interface “Payroll address” 18.12.6.3 vlan 255
-> ip interface “Human Resources” 10.200.12.101 vlan 500 no forward snap
-> ip interface Distribution 11.255.14.102 vlan 500 local-proxy-arp primary
-> no ip interface Marketing
-> vrf 100 no ip interface “Payroll address”

-> ip interface l3-vpn address 10.1.1.1/24 service 10
-> service 10 vlan-xlation disable
ERROR: Modify vlan translation currently not allowed for service (10)
-> vrf 100 ip interface l3-vpn100 address 100.1.1.1/24 service 20
-> no ip interface l3-vpn
-> vrf 100 no ip interface l3-vpn100

Release History

Release 7.1.1; command introduced
Release 8.4.1.R03; service parameter added to support binding an SPB service to an IP interface.
Release 8.5R4; service parameter support for binding an L2 GRE tunneling service to an IP interface added. Support for an IP interface on an SPB Control BVLAN added.

Related Commands

show ip interface Displays the status and configuration of IP interfaces.

MIB Objects

alaIpInterfaceTable
  alaIpInterfaceName
  alaIpInterfaceAddress
  alaIpInterfaceVipAddress
  alaIpInterfaceMask
  alaIpInterfaceAdminState
  alaIpInterfaceDeviceType
  alaIpInterfaceVlanID
  alaIpInterfaceServiceID
  alaIpInterfaceIpForward
  alaIpInterfaceEncap
  alaIpInterfaceLocalProxyArp
  alaIpInterfacePrimCfg
  alaIpInterfaceOperState
  alaIpInterfaceOperReason
  alaIpInterfaceRouterMac
  alaIpInterfaceBcastAddr
  alaIpInterfacePrimAct
**ip interface rtr-port**

Configures an IP routed-port interface by associating an IP interface with a port or link aggregate and a VLAN.

```
ip interface if_name address ip_address/mask vlan vlan_id rtr-port {port chassis/slot/port | linkagg agg_id} {tagged | untagged}
```

### Syntax Definitions

- **if_name**: A unique name for the IP interface. Use quotes around the string if the name contains multiple words with spaces between them (for example, “ALE Marketing”). This value is case sensitive.
- **ip_address**: IP host address to specify this IP interface.
- **mask**: IP mask to specify this IP interface.
- **vlan_id**: An unused VLAN ID to which this IP interface is associated.
- **chassis/slot/port**: The chassis ID, slot, and port number (1/1/3) of the physical port to bind to the IP interface.
- **agg_id**: The link aggregate ID to bind to the IP interface.
- **tagged**: Whether the assigned port or link aggregate is tagged for the specified VLAN.
- **untagged**: Whether the assigned port or link aggregate is untagged for the specified VLAN.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- In a single step, this command creates the specified VLAN, configures an IP interface for the VLAN, and assigns a port or link aggregate (tagged or untagged) to the VLAN.

- Configuring an IPv4 and IPv6 routed-port interface for the same VLAN ID is supported if the following conditions are met:
  - The VLAN ID, port, and the tagged/untagged port status for both interfaces is the same (for example, IPv4 and IPv6 routed interfaces are both bound to VLAN 850 with port 1/1/2 tagged).
  - Both interfaces are configured in the same VRF instance.
• Make sure the specified VLAN ID does not already exist in the switch configuration or is only used as a routed-port VLAN for an IPv4 interface. This VLAN will serve as a routing-only VLAN with a single port or link aggregate (Layer 2 functionality is not supported).

• Make sure the specified port or link aggregate is not already assigned to a VLAN that is not a routed-port VLAN. However, the port or link aggregate can be assigned to other routed-port VLANs.

• Attempting to add more ports or link aggregates to the routed-port VLAN or attempting to delete the VLAN is not allowed. The VLAN can only be removed by deleting the associated IPv4 and, if configured, the associated IPv6 interface.

• The same VLAN cannot be used for both a routed-port interface and a non-routed-port interface.

• Once configured, an IP routed-port interface is operationally equivalent to an IP VLAN interface. Routing protocols and other switch features that use IP are configured and operate on an IP routed-port interface in the same manner as on a regular IP interface.

Examples

-> ip interface "rp-vlan30" 10.0.0.1/8 vlan 30 rtr-port port 1/1/1 tagged
-> ip interface "rp-vlan40" 20.0.0.1/8 vlan 40 rtr-port port 1/1/2 untagged
-> ip interface "rp-vlan50" 30.0.0.1/8 vlan 40 rtr-port linkagg 6 tagged
-> ip interface "rp-vlan60" 40.0.0.1/8 vlan 50 rtr-port linkagg 7 untagged

-> vlan 70
-> ip interface rp-vlan70 rtr-port port 1/1/13 untagged vlan 70
ERROR: vlan 70 already present

-> ip interface rpv4-vlan rtr-port port 1/1/11 tagged vlan 300
-> ipv6 interface rpv6-vlan rtr-port port 1/1/11 tagged vlan 300

-> no ipv6 interface rpv6-vlan
-> ipv6 interface rpv6-vlan rtr-port port 1/1/13 untagged vlan 300
ERROR: Configuration conflict with IPv4 routed port interface rpv4-vlan

Release History

Release 7.3.4; command introduced

Related Commands

show ip interface Displays the status and configuration of IP interfaces.

MIB Objects

alaIpInterfaceTable
  alaIpInterfaceName
  alaIpInterfaceVlanID
  alaIpInterfaceDeviceType
  alaIpInterfacePortIfindex
  alaIpInterfaceTag
ip interface tunnel

Configures the end points for a GRE or IPIP tunnel.

```
ip interface if_name tunnel [source ip_address] [destination ip_address] [protocol {ipip | gre}]
```

### Syntax Definitions

- **if_name**: Text string. Use quotes around string if description contains multiple words with spaces between them (for example, “ALE Marketing”). This value is case sensitive.
- **source ip_address**: Source IP address of the tunnel.
- **destination ip_address**: Destination IP address of the tunnel.
- **ipip**: Specifies the tunneling protocol as IPIP.
- **gre**: Specifies the tunneling protocol as GRE.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipip</td>
<td>ipip</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You can configure an interface as either a VLAN or tunnel interface.

### Examples

```
-> ip interface “tnl-1” tunnel source 23.23.23.1 destination 155.2.2.2 protocol gre
-> ip interface “tnl-1” tunnel source 23.23.23.1 destination 155.2.2.2 protocol ipip
```

### Release History

Release 7.1.1; command introduced
**Related Commands**

*show ip interface*  
Displays the status and configuration of IP interfaces.

**MIB Objects**

alaIpInterfaceTable

- alaIpInterfaceName
- alaIpInterfaceTunnelSrc
- alaIpInterfaceTunnelDst
- alaIpInterfaceDeviceType
**ip interface dhcp-client**

Configures a DHCP client IP interface that is to be assigned an IP address from a DHCP server.

```
ip interface dhcp-client [vlan vlan_id] [vsi-accept-filter filter-string] [server-preference] [release | renew] [option-60 opt60_string] [admin {enable | disable}] [local-proxy-arp | no local-proxy-arp]
no ip interface dhcp-client
```

**Syntax Definitions**

- **dhcp-client**: Reserved IP interface name indicating this interface use DHCP to obtain an IP address from a DHCP server.
- **vlan_id**: An existing VLAN ID number (1–4094).
- **filter-string**: String that matches with option-43 filed of the DHCPACK to prefer the desired OXO server. By default the filter-string will be empty string (“ “).
- **server-preference**: Enables DHCP server precedence logic. The DHCP server preference logic is mutually exclusive with vsi-accept-filter.
- **release**: Releases the DHCP server assigned IP address.
- **renew**: Renews the DHCP server assigned IP address.
- **opt60_string**: The option-60 field value to be included in DHCP discover/request packets.
- **enable**: Enables the administrative status for the IP interface.
- **disable**: Disables the administrative status for the IP interface.
- **local-proxy-arp**: Enables Local Proxy ARP on the specified interface.
- **no local-proxy-arp**: Disables Local Proxy ARP on the specified interface.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>opt60_string</td>
<td>OmniSwitch-xxxx (xxxx = Platform, for example, 6900)</td>
</tr>
</tbody>
</table>
| enable | disable
| filter-string     | (“ “). |
| server-preference | disabled |
| local-proxy-arp | no local-proxy-arp |
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to remove the DHCP-client IP interface.
- Only one DHCP client IP interface can be assigned per switch but it can belong to any VLAN and any VRF instance.
- The time zone and the system name of the OmniSwitch is set according to the time zone (DHCP Option-2) and system name (DHCP Option-12) assigned by the DHCP server. DHCP server sets the Option-2 and Option-12 values only when they are set to their default values on bootup or they are already set by the DHCP. Once the user configures these values to non-default values, DHCP does not set them.
  - **TimeZone (DHCP Option-2)**
    - The system time zone, if configured by the user (through CLI, WebView, SNMP) will always override the one obtained through Option-2.
    - The ‘show system’ command output shows the current time zone that is effective.
    - On deletion of the DHCP client IP interface, the timezone will move back to the default time zone of UTC.
    - If the user configured timezone is deleted using ‘system timezone’ command, then the time zone obtained through DHCP is considered, if any. Otherwise, it will move back to the default timezone of UTC.
    - Setting of time zone by DHCP option-2 is independent of NTP. NTP does not manage timezones, instead it manages all time information based on UTC.
    - Option-2 value will be set by DHCP only if it corresponds to the timezone supported by AOS. Otherwise, this offset will be silently ignored. Refer to the *OmniSwitch AOS Release 8 Switch Management Guide* for a list of supported time zone.
  - **System name (DHCP Option-12)**
    - The system name, if configured by the user (through CLI, WebView, SNMP) will always override the one obtained through Option-12.
    - The configuration snapshot will not change, if the system name is already explicitly configured by the user.
    - The ‘show system’ command shows the current system name that is effective.
    - On deletion of the DHCP client IP interface, the system name will move back to the default system name.
    - If the user configured system name is deleted using ‘system name’ command, then the system name obtained through DHCP is considered, if any. Otherwise, it will move back to the default system name.
- The minimum lease time accepted on the DHCP-client interface is 5 minutes.
• The VSI filter-string once configured cannot be deleted. It can be overwritten or modified. It can be configured as empty string (“ ”).

• The VSI accept filter is case-sensitive. The maximum length of a vsi-accept-filter can be of 64 character length.

• In order to retain the same OXO server which was configured before RCL, the VSI filter must match the hard coded string “alcatel.a4400.0”.

• DHCP client preference to obtain the lease from the highest priority server among the multiple offers received can be enabled using the server-preference option.

• Server preference option can also be set without specifying VLAN ID, provided the dhcp-client interface is associated with a VLAN prior to setting the server preference.

• The server-preference option is mutually exclusive with vsi-accept-filter option.

• Use the no server-preference option to remove the server preference.

Examples

-> ip interface dhcp-client vlan 100
-> ip interface dhcp-client admin enable
-> ip interface dhcp-client release
-> ip interface dhcp-client renew
-> ip interface dhcp-client option-60 OmniSwitch
-> no ip interface dhcp-client
-> ip interface dhcp-client vsi-accept-filter “alcatel.a4400.0”
-> ip interface dhcp-client vlan 1 server-preference
-> ip interface dhcp-client server-preference
-> ip interface dhcp-client no server-preference

Release History

Release 7.3.4; command introduced.
Release 8.5R1; server-preference parameters included.

Related Commands

show ip interface Displays the status and configuration of IP interfaces.

MIB Objects

alaIpInterfaceTable
alaIpInterfaceDhcpStatus
alaIpInterfaceDhcpIpRelease
alaIpInterfaceDhcpIpRenew
alaIpInterfaceDhcpOption60String
alaIpInterfaceDhcpVsiAcceptFilterString
alaIpInterfaceDhcpServerPreference
ip router primary-address

Configures the router primary IP address. By default, the router primary address is derived from the first IP interface that becomes operational on the router.

**Syntax Definitions**

`ip_address`  
32-bit IP address.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The router primary address must be a valid IP unicast host address.
- The router primary IP address is used by BGP to derive its unique BGP Identifier, if the router router-id is not a valid IP unicast address.
- It is recommended that the primary address be explicitly configured on dual CMM chassis.

**Examples**

```
-> ip router primary-address 172.22.2.115
```

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- `ip router router-id`  
  Configures the router ID for the router.

**MIB Objects**

alaDcrTmConfig

alaDrcTmIpRouterPrimaryAddress
**ip router router-id**

Configures the router ID for the router. By default, the router primary address of the router is used as the router ID. However, if a primary address has not been explicitly configured, the router ID defaults to the address of the first IP interface that becomes operational.

**ip router router-id ip_address**

---

**Syntax Definitions**

```
ip_address
```

32-bit IP address.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The router ID can be any 32-bit number.
- If the router ID is not a valid IP unicast host address, the BGP identifier is derived from the router primary address.
- It is recommended that the router ID be explicitly configured on dual CMM chassis.
- The router ID is used by OSPF and BGP for unique identification of the router in the network.

**Examples**

```
-> ip router router-id 172.22.2.115
```

**Release History**

Release 7.1.1; command introduced
Related Commands

```
ip router primary-address
```
Configures the router primary IP address.

MIB Objects

```
alaDcrTmConfig
  alaDrcTmIpRouterId
```
**ip static-route**

Creates or deletes an IP static route. Static routes are user-defined; they carry a higher priority than routes created by dynamic routing protocols. By default, static routes carry a higher priority than the dynamic routes.

```
ip static-route ip_address [mask mask] [gateway {gateway_address | null}] [tag num] [name string] | interface interface_name | follows ip_address] [metric metric]
```

```
no ip static-route ip_address [mask mask] [gateway {gateway_address | null}] | interface interface_name | follows ip_address] [metric metric]
```

**Syntax Definitions**

- `ip_address` Destination IP address of the static route.
- `mask` Subnet mask corresponding to the destination IP address.
- `gateway gateway_address` IP address of the next hop used to reach the destination IP address.
- `gateway null` Use this option to configure an IPv4 blackhole route.
- `tag num` Tag to be used for route.
- `name string` Name to be used for route.
- `interface interface_name` Interface of the next hop used to reach the destination IP address.
- `follows ip_address` The recursive static route follows this IP address. The recursive route uses the same gateway (and interface) or nexthop that is used to reach this host address.
- `metric` Metric or cost (hop count) for the static route. You can set a priority for the static route by assigning a metric value. The lower the metric value, the higher the priority. Valid range is 1–15.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- By default, static routes have a higher priority over dynamic routes; however, it can be changed using the `ip route-pref` command.

- Static routes do not age out of the routing tables; however, they can be deleted. Use the no form of this command to delete a static route.

- A static route is active if the interface it is using is “UP”.

- The subnet mask is not required if you want to use the natural subnet mask. By default, the switch imposes a natural mask on the IP address.

- If directly connected, NAT routers interface name can be used instead of gateway IP address, provided the router is enabled for proxy-ARP to handle ARP requests for the route addresses.

- Use the `null` option to configure IPv4 blackhole routes. A blackhole route is used to forward unwanted traffic to a blackhole.
  - Redistribution of blackhole routes is supported. Dynamic routing protocols may advertise these routes, but the gateway associated with the route(s) will be an address on the router advertising them.
  - Leaking of blackhole routes across SPB service backbones is supported. However, blackhole routes cannot be leaked between VRFs. Blackhole routes need to be explicitly configured using the `ip static-route` command in any/all VRFs.
  - Blackhole routes are created and installed through static route commands. Dynamic Routing protocols shall not install blackhole IP routes.
  - Blackhole routes shall never be part of ECMP.
  - Blackhole routes cannot be enabled for BFD support.

- Alternatively, the gateway address ‘0.0.0.0’ can be used to create an IPv4 blackhole route.

Examples

-> ip static-route 171.11.1.0/24 gateway 171.11.2.1
-> ip static-route 171.11.1.0/24 interface Int1
-> ip static-route 12.0.0.0/8 interface Int1
-> ip static-route 171.11.1.0/24 follows 192.168.10.1
-> ip static-route 55.0.0.0/8 gateway null
-> ip static-route 55.0.0.0/8 gateway 0.0.0.0

Release History

Release 7.1.1; command introduced
Release 7.3.4; interface, tag, name parameters included
Release 8.6R1; null keyword added.

Related Commands

- `ip route-pref` Configures the route preference of a router.
- `show ip routes` Displays the IP Forwarding table.
- `show ip router database` Displays a list of all routes (static and dynamic) that exist in the IP router database.
- `show ip route-pref` Displays the IPv4 routing preferences of a router.
MIB Objects

alaIprmStaticRoute
  alaIprmStaticRouteDest
  alaIprmStaticRouteMask
  alaIprmStaticRouteNextHop
  alaIprmStaticRouteTag
  alaIprmStaticRouteName
  alaIprmStaticRouteMetric
  alaIprmStaticRouteStatus
  alaIprmStaticRouteType
**ip static-route all bfd-state**

Enables BFD for all IPv4 static routes.

```
ip static-route all bfd-state {enable| disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for all IPv4 static routes.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for all IPv4 static routes.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When there are static routes configured in the switch, BFD is enabled to track the gateway.
- If the route is not reachable, it will be moved to the inactive database.

### Examples

```
-> ip static-route all bfd-state enable
-> ip static-route all bfd-state disable
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **ip static-route bfd-state** Enables BFD for a specific static route.
- **show ip router database** Displays a list of all routes (static and dynamic) that exist in the IP router database.

### MIB Objects

- alaIprmConfig
- alaIprmStaticAllBfd
ip static-route bfd-state

Enables or disables BFD for a specific IPv4 static route.

```
ip static-route ipv4_prefix/pfx_length gateway ipv4_host_address bfd-state {enable| disable}
```

**Syntax Definitions**

- `ipv4_prefix` The destination IPv4 address.
- `pfx_length` The prefix length for the destination IP address.
- `ipv4_host_address` The gateway IPv4 address.
- `enable` Enables BFD for the IPv4 static route.
- `disable` Disables BFD for the IPv4 static route.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

BFD is enabled to track the gateway of static routes.

**Examples**

```
-> ip static-route 192.100.1.0/24 gateway 100.1.1.10 bfd-state enable
-> ip static-route 192.100.1.0/24 gateway 100.1.1.10 bfd-state disable
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip static-route all bfd-state` Enables BFD for all static routes.
- `show ip router database` Displays a list of all routes (static and dynamic) that exist in the IP router database.
**MIB Objects**

alaIprmStaticRouteTable
  alaIprmStaticRouteDest
  alaIprmStaticRouteMask
  alaIprmStaticRouteNextHop
  alaIprmStaticRouteBfdStatus
  alaIprmStaticRouteType
**ip route-pref**

Configures the route preference of a router.

```
[vrf vrf_name] ip route-pref {spb-mgmt | static | ospf | isisl2 | isisl1 | rip | ebgp | ibgp | import} value
```

### Syntax Definitions

- **vrf name**: The alphanumeric name (1–20 characters) assigned to the VRF instance.
- **static**: Configures the route preference for static routes.
- **ospf**: Configures the route preference for OSPF routes.
- **isisl1**: Configures the route preference for ISIS L1 routes.
- **isisl2**: Configures the route preference for ISIS L2 routes.
- **rip**: Configures the route preference for RIP routes.
- **spb-mgmt**: Configures the route preference for SPB management routes.
- **ebgp**: Configures the route preference for external BGP routes.
- **ibgp**: Configures the route preference for internal BGP routes.
- **import**: Configures the route preference for the routes that are imported.

**value**: Route preference value.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static value</td>
<td>2</td>
</tr>
<tr>
<td>ospf value</td>
<td>110</td>
</tr>
<tr>
<td>isisl1 value</td>
<td>115</td>
</tr>
<tr>
<td>isisl2 value</td>
<td>118</td>
</tr>
<tr>
<td>rip value</td>
<td>120</td>
</tr>
<tr>
<td>spb-mgmt value</td>
<td>150</td>
</tr>
<tr>
<td>ebgp value</td>
<td>190</td>
</tr>
<tr>
<td>ibgp value</td>
<td>200</td>
</tr>
<tr>
<td>import value</td>
<td>210</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Route preference of local routes cannot be changed.
- Make sure the route preference configured for SPB management (SPB-MGMT) routes does not conflict with the route preference configured for any other protocols.

Note. When using ISSU to upgrade the switch, ISSU will automatically change the SPB-MGMT route preference to the next lowest value below 150 if there is a conflict with another protocol previously configured with the same route preference value. After an ISSU upgrade, use the write memory command to ensure any changes are retained.

Examples

- ip route-pref ebgp 20
- ip route-pref rip 60
- ip route-pref import 210

Release History

Release 7.1.1; command introduced
Release 7.3.1; vrf and import parameters added.
Release 8.7R2; spb-mgmt parameter added.

Related Commands

show ip route-pref Displays the configured route-preference of a router.
ip import Configures a route map to import routes from GRT to the destination VRF.
show ip import Displays the import route configuration details.

MIB Objects

alaIprmRtPrefTable
  alaIprmRtPrefEntryType
  alaIprmRtPrefEntryValue
**ip default-ttl**

Configures the Time To Live (TTL) for IP packets. The TTL value is the maximum number of hops an IP packet travels before being discarded.

```plaintext
ip default-ttl hops
```

**Syntax Definitions**

`hops`  
TTL value, in hops. Valid range is 1–255.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hops</td>
<td>64</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This value represents the default value inserted into the TTL field of the IP header for datagrams originating from this switch whenever a TTL value is not supplied by the transport layer protocol.

**Examples**

```plaintext
-> ip default-ttl 30
```

**Release History**

Release 7.1.1; command introduced

**Related Commands**

| show ip config | Displays IP configuration parameters. |

**MIB Objects**

IpDefaultTTL
ping

Tests whether an IP destination can be reached from the local switch. This command sends an ICMP echo request to a destination and then waits for a reply. To ping a destination, enter the `ping` command and enter either the IP address or hostname of the destination. The switch pings the destination using the default frame count, packet size, interval, and timeout parameters (6 frames, 64 bytes, 1 second, and 5 seconds respectively). You can also customize any or all of these parameters as described below.

```
ping {ip_address | hostname} [source-interface ip_interface] [count count] [size packet_size] [interval seconds] [timeout seconds] [data-pattern string] [dont-fragment] [tos tos_val]
```

**Syntax Definitions**

- **ip_address**
  IPv4 address of the system to ping.

- **hostname**
  DNS name of the system to ping.

- **source-interface ip_interface**
  IP address or interface name to use as the source IP for the ping packets.

- **count**
  Number of frames to be transmitted.

- **packet_size**
  Size of the data portion of the packet sent for this ping, in bytes. Valid range is 1–65507.

- **interval seconds**
  Polling interval. The switch polls the host at time intervals specified in seconds.

- **timeout seconds**
  Number of seconds the program waits for a response before timing out.

- **data-pattern string**
  The data pattern to be used in the data field of the ping packets.

- **dont-fragment**
  Sets the don't-fragment bit in the IP packet.

- **tos tos_val**
  Type of Service field in the IP header.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>6</td>
</tr>
<tr>
<td>packet_size</td>
<td>64</td>
</tr>
<tr>
<td>interval seconds</td>
<td>1</td>
</tr>
<tr>
<td>timeout seconds</td>
<td>5</td>
</tr>
<tr>
<td>dont-fragment</td>
<td>0</td>
</tr>
<tr>
<td>tos tos_val</td>
<td>0</td>
</tr>
<tr>
<td>data-pattern string</td>
<td>Repeating sequence of ASCII characters 0x4 onwards to 0xff</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you change the default values, they are only applied to the current ping. The next time you use the ping command, the default values are used unless you again enter different values.

Examples

-> ping 10.255.11.242

PING 10.255.11.242: 56 data bytes
64 bytes from 10.255.11.242: icmp_seq=0. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=1. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=2. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=3. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=4. time=0. ms
64 bytes from 10.255.11.242: icmp_seq=5. time=0. ms
-----10.255.11.242 PING Statistics-----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0

-> ping 10.0.0.1 source-interface mgmt
-> ping 10.0.0.1 tos 1
-> ping 10.0.0.1 timeout 10
-> ping 10.0.0.1 interval 10
-> ping 10.0.0.1 dont-fragment
-> ping 10.0.0.1 data-pattern AB

Release History

Release 7.1.1; command introduced

Related Commands

traceroute

Finds the path taken by an IP packet from the local switch to a specified destination.

MIB Objects

N/A
**traceroute**

Finds the path taken by an IP packet from the local switch to a specified destination. This command displays the individual hops to the destination as well as some timing information.

```
traceroute {ip_address | hostname} [max-hop max_hop_count] [min-hop min_hop_count] [source-interface ip_interface] [probes probe_count] [timeout seconds] [port port_number_value]
```

**Syntax Definitions**

- `ip_address` IPv4 address of the host whose route you want to trace.
- `hostname` DNS name of the host whose route you want to trace.
- `max_hop_count` Maximum hop count for the trace. The valid range is 1–255.
- `min_hop_count` Minimum hop count for the trace. The valid range is 1–30.
- `ip_interface` Source IP interface to be used in the traceroute packets.
- `probe_count` The number of packets (retry) sent for each hop-count. The valid range is 1–10000.
- `seconds` The time to wait for the response of each probe packet.
- `port_number_value` The destination port number to be used in the probing packets.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max-hop</code> <code>max_hop_count</code></td>
<td>30</td>
</tr>
<tr>
<td><code>min-hop</code> <code>min_hop_count</code></td>
<td>1</td>
</tr>
<tr>
<td><code>source-interface</code> <code>ip_interface</code></td>
<td>Outgoing IP interface as per route lookup</td>
</tr>
<tr>
<td><code>probes</code> <code>probe_count</code></td>
<td>3</td>
</tr>
<tr>
<td><code>timeout</code> <code>seconds</code></td>
<td>5</td>
</tr>
<tr>
<td><code>port</code> <code>port_number_value</code></td>
<td>33334</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

When using this command, you must enter the name of the destination as part of the command line (either the IP address or host name).

**Examples**

-> traceroute 128.251.17.224

traceroute to 128.251.17.224, 30 hops max, 40 byte packets
1  10.255.11.254 0 ms 0 ms 0 ms
2  172.23.0.251 0 ms 16.6667 ms 0 ms
3  128.251.14.253 0 ms 0 ms 0 ms
4  128.251.17.224 0 ms 0 ms 0 ms

-> traceroute 128.251.17.224 max-hop 3
traceroute to 128.251.17.224, 3 hops max, 40 byte packets
1  10.255.11.254 0 ms 0 ms 0 ms
2  172.23.0.251 16.6667 ms 0 ms 0 ms
3  128.251.14.253 0 ms 0 ms 0 ms

-> traceroute 10.0.0.1 source-interface mgmt
-> traceroute 10.0.0.1 min-hop 3
-> traceroute 10.0.0.1 probes 3
-> traceroute 10.0.0.1 timeout 10
-> traceroute 10.0.0.1 port-number 1025

**Release History**

Release 7.1.1; command introduced

**Related Commands**

*show ip routes* Displays the IP Forwarding table.

**MIB Objects**

* N/A
ip directed-broadcast

Enables or disables IP directed broadcasts routed through the switch. An IP directed broadcast is an IP datagram that has all zeros or all 1s in the host portion of the destination address. The packet is sent to the broadcast address of a subnet to which the sender is not directly attached.

[vrf vrf_name] ip directed-broadcast {enable | disable}

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf_name</td>
<td>The name of an existing VRF instance.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables IP directed broadcasts.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables IP directed broadcasts.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
</tr>
<tr>
<td>6900V72/C32</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Directed broadcasts are used in denial-of-service attacks. In a DoS attack, a continuous stream of ping requests are sent from a falsified source address to a directed broadcast address. This results in a large stream of replies, which can overload the host of the source address. By default, the switch drops directed broadcasts. Directed broadcasts must not be enabled.

- When IP directed broadcast is enabled, by default, it is enabled on the 'default' VRF.

### Examples

- `-> ip directed-broadcast enable`
- `-> ip directed-broadcast disable`

### Release History

Release 7.1.1; command introduced
Related Commands

show ip directed-broadcast  Displays the status of the directed broadcast configuration and trusted source IP address configuration.

MIB Objects

alaIpDirectedBroadcast
**ip directed-broadcast trusted-source-ip**

Specify the source IP address, destination IP address and destination VLAN information to broadcast the packets in controlled manner. The specified information is considered as the trusted information to broadcast the packets received from the defined parameters, and the remaining broadcast packets are dropped.

```bash
[vrf vrf_name] ip directed-broadcast trusted-source-ip {ip_address/mask | ip_address mask
subnet_mask} [destination-ip {ip_address/mask | ip_address destination-mask subnet_mask}] [destination-vlan {vlan_id | vlan_id|vlan_id}]
```

```bash
[vrf vrf_name] no ip directed-broadcast trusted source-ip ip_address {ip_address/mask | ip_address mask subnet_mask}
```

**Syntax Definitions**

- `vrf_name` (The name of an existing VRF instance.)
- `trusted-source-ip ip_address` (Source IP address from which the broadcast packets are received.)
- `destination-ip ip_address` (Destination address to which the packets must be directed.)
- `subnet_mask` (The source mask from which the broadcast packets are received.)
- `destination-mask subnet_mask` (The destination mask to which the packets must be directed.)
- `vlan_id` (Existing VLAN ID to which the packets are to be directed.)

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_address</code></td>
<td>0.0.0.0</td>
</tr>
<tr>
<td><code>subnet_mask</code></td>
<td>IP address class/0.0.0.0</td>
</tr>
<tr>
<td><code>vlan_id</code></td>
<td>None</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` command to remove the trusted information configured with the source IP address for controlled IP directed broadcast.
- IP directed broadcast must be enabled for the controlled IP directed broadcast to work.
- When controlled IP directed broadcast is enabled, by default, it is enabled on the ‘default’ VRF.
- The trusted information must have the source IP with optional destination IP address or VLAN ID.
- Ensure that the configured address/mask combination (source/destination IP address) configuration is not a subset of an already existing address/mask.
- If the source IP matches, then the packets are broadcasted in the particular destination IP interface or VLAN interfaces. The remaining packets are dropped.
- When the packet received matches with the source IP and if the destination IP or destination VLAN information are not defined by the user, then the packet will be forwarded based on the routing information in the switch.
- If no source IP is provided as trusted, by default, all the packets are forwarded.
- If the destination IP or VLAN is defined by the user, then the destination address of the packet will be matched with the user defined list and routes the packets if the destination IP matches. If the VLAN information is defined, then the packets will be routed if the destination VLAN matches a VLAN in the configured allowed VLAN list. If neither the destination IP or VLAN matches the ones configured, the packet are dropped.
- If the destination IP is not reachable or if the destination subnet is not directly connected, packet will be dropped.
- If the directed broadcast is set to controlled mode and the user does not specify any trusted information, all the broadcast packets will be dropped. This case is equivalent to disabled state of directed-broadcast.
- 32 source IP addresses can be defined, and each source IP address can have 30 destination IP addresses and 30 destination VLAN IDs.
- If IP directed broadcasts is disabled using the command `ip directed-broadcast disable`, which also is the default, all packets with subnet broadcast, will be dropped.

**Examples**

- `ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0`
- `vrf test123 ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0 destination-ip 10.0.0.255 destination-mask 255.255.255.255`
- `ip directed-broadcast trusted-source-ip 30.0.0.0/24 destination-ip 10.0.0.255/24`
- `ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0 destination-vlan 10`
- `ip directed-broadcast trusted-source-ip 30.0.0.0/24 destination-vlan 10-15`
- `no ip directed-broadcast trusted-source-ip 30.0.0.0/24`
- `no ip directed-broadcast trusted-source-ip 30.0.0.0 mask 255.255.255.0`

**Release History**

Release 8.5R2; command introduced.
Related Commands

**ip directed-broadcast**  Enables or disables IP directed broadcasts routed through the switch.

**ip directed-broadcast clear**  Clears all the trusted information configured.

**show ip directed-broadcast**  Displays the status of the directed broadcast configuration and trusted source IP address configuration.

MIB Objects

alaIpDirectedBroadcastCtrlSrcTable
   alaIpDirectedBroadcastCtrlSrcAddrType
   alaIpDirectedBroadcastCtrlSrcAddr
   alaIpDirectedBroadcastCtrlSrcMask
alaIpDirectedBroadcastCtrlDstTable
   alaIpDirectedBroadcastCtrlDstAddrType
   alaIpDirectedBroadcastCtrlDstAddr
   alaIpDirectedBroadcastCtrlDstMask
alaIpDirectedBroadcastCtrlVlanTable
   alaIpDirectedBroadcastCtrlVlanID
**ip directed-broadcast clear**

Clears all the trusted information configured.

```
[vrf vrf_name] ip directed-broadcast clear [trusted-source-ip {ip_address/mask | ip_address mask subnet_mask}]
```

**Syntax Definitions**

- **vrf_name**: The name of an existing VRF instance.
- **trusted-source-ip ip_address**: Source IP address from which the broadcast packets are received.
- **subnet_mask**: The source mask from which the broadcast packets are received.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the source IP is specified, then the destination and the VLAN information for the source IP specified is cleared. If the command is specified without the source IP address, entire trusted information database is cleared.

**Examples**

```
-> ip directed-broadcast clear
-> ip directed-broadcast clear trusted-source-ip 20.20.0 mask 255.255.255.0
```

**Release History**

Release 8.5R2; command introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip directed-broadcast</code></td>
<td>Enables or disables IP directed broadcasts routed through the switch.</td>
</tr>
<tr>
<td><code>ip directed-broadcast trusted-source-ip</code></td>
<td>Specify the source IP address, destination IP address and destination VLAN information to broadcast the packets in controlled manner.</td>
</tr>
</tbody>
</table>

### MIB Objects

alaIpDirectedBroadcastCtrlSrcTable
- alaIpDirectedBroadcastCtrlSrcAddrType
- alaIpDirectedBroadcastCtrlSrcAddr
- alaIpDirectedBroadcastCtrlSrcMask
- alaIpDirectedBroadcastCtrlSrcClear

alaIpDirectedBroadcastCtrlGlobalConfig
- alaIpDirectedBroadcastCtrlClearAll
**show ip directed-broadcast**

Displays the status of the directed broadcast configuration and trusted source IP address configuration.

```
[vrf vrf_name] show ip directed-broadcast [trusted-source-ip {ip_address/mask | ip_address mask subnet_mask}] details
```

**Syntax Definitions**

- `vrf_name`: The name of an existing VRF instance.
- `trusted-source-ip ip_address`: Source IP address from which the broadcast packets are received.
- `subnet_mask`: The source mask from which the broadcast packets are received.
- `details`: Displays the destination IP address or VLAN information for the specified source IP.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use `details` keyword to view the destination IP addresses or VLANs information for the specified source IP.

**Examples**

```
-> show ip directed-broadcast
IP Directed Broadcast is enabled
Source-IP       MASK       Destination-IP VLAN
-----------------+------------+--------------+-----
100.10.1.0       255.255.255.0     YES            NO
100.10.2.2       255.255.255.255   YES            NO
100.10.3.0       255.255.255.224   YES            NO
100.10.4.0       255.255.255.248   YES            NO

-> show ip directed-broadcast trusted-source-ip 10.10.10.0 mask 255.255.255.0 details
Source-IP/Mask    =  10.10.10.0/255.255.255.0
Destination-IP/Mask =  20.20.20.0/255.255.255.0,
Vlan              =  10
```
**output definitions**

<table>
<thead>
<tr>
<th>Source-IP/Mask</th>
<th>Trusted source IP address and mask configured in a controlled manner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination-IP/Mask</td>
<td>Trusted destination IP address and mask configured in a controlled manner.</td>
</tr>
<tr>
<td>Vlan</td>
<td>Trusted VLAN ID configured for directed broadcast in a controlled manner.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- `ip directed-broadcast` Enables or disables IP directed broadcasts routed through the switch.
- `ip directed-broadcast trusted-source-ip` Specify the source IP address, destination IP address and destination VLAN information to broadcast the packets in controlled manner.

**MIB Objects**

N/A
ip service

Enables (opens) or disables (closes) well-known or user-defined TCP/UDP service ports. Selectively enabling or disabling these types of ports provides an additional method for protecting against unauthorized switch access or Denial of Service (DoS) attacks.

[vrf vrf_name] ip service {all | service_name | port service_port} admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>vrf_name</th>
<th>The name of an existing VRF instance in which services are to be enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Configures access to all TCP/UDP ports.</td>
</tr>
<tr>
<td>service_name</td>
<td>The name of the TCP/UDP service to enable or disable. (Refer to the table in the “Usage Guidelines” section for a list of supported service names.)</td>
</tr>
<tr>
<td>service_port</td>
<td>A TCP/UDP service port number. Configures access by port number rather than by service name. (Refer to the table in the “Usage Guidelines” section for a list of well-known port numbers.) If a user-defined port number is specified, the valid range is 20000–20999.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables access to the service.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables access to the service.</td>
</tr>
</tbody>
</table>

Defaults

All TCP/UDP ports are open by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command only applies to TCP/UDP service ports opened by default. It does not affect ports that are opened by applications, such as RIP, BGP, and so on.
- Use the all option with this command to configure access to all well-known TCP/UDP service ports.
- To designate which port to enable or disable, specify either the name of a service or the well-known port number associated with that service. Specifying a name and a port number in a single command line is not supported.
- When using service names, it is possible to specify more than one service in a single command line by entering each service name separated by a space. See the “Example” section for more information.
- When specifying a service port number, the `port` keyword is required and that only one port number is allowed in a single command.

- The following table lists the `ip service` command options for specifying TCP/UDP services and also includes the well-known port number associated with each service:

<table>
<thead>
<tr>
<th>service name</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>21</td>
</tr>
<tr>
<td>ssh</td>
<td>22</td>
</tr>
<tr>
<td>telnet</td>
<td>23</td>
</tr>
<tr>
<td>http</td>
<td>80</td>
</tr>
<tr>
<td>https</td>
<td>443</td>
</tr>
<tr>
<td>ntp</td>
<td>123</td>
</tr>
<tr>
<td>snmp</td>
<td>161</td>
</tr>
</tbody>
</table>

- If a VRF is specified, the service is enabled or disabled in the specified VRF. By default, the services are enabled in the ‘default’ VRF.

**Examples**

- `-> ip service all admin-state disable`
- `-> ip service ftp admin-state enable`
- `-> ip service port 20000 admin-state enable`
- `-> vrf vrf1 ip service ftp admin-state enable`

**Release History**

Release 7.1.1; command introduced
Release 7.3.1; `vrf` parameter added.

**Related Commands**

- `ip service port` Configures a user-defined TCP/UDP port for the specified service.
- `show ip service` Displays the IP service TCP/UDP port configuration and status.

**MIB Objects**

- `alaIpServiceTable`
  - `alaIpServiceType`
  - `alaIpServicePort`
  - `alaIpServiceStatus`
- `alaIpPortServiceTable`
  - `alaIpPortServicePort`
  - `alaIpPortServiceStatus`
**ip service port**

Configures a user-defined TCP/UDP service port for the specified service.

```
ip service {service_name} port {default | service_port}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>service_name</th>
<th>The name of the TCP/UDP service to enable or disable. (Refer to the table in the “Usage Guidelines” section for a list of supported service names.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_port</td>
<td>A TCP/UDP service port number (Refer to the table in the “Usage Guidelines” section for a list of supported service names.) Valid range is the default service port number or 20000-20999.</td>
</tr>
<tr>
<td>default</td>
<td>Sets the port back to the well-known port for the specified service.</td>
</tr>
</tbody>
</table>

### Defaults

By default, the service uses the well-known TCP/UDP port number for that service.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `default` parameter with this command to set the port for the specified service back to the well-known default port for that service. For example, if the FTP port was previously changed to “20000”, then the `ip service ftp port default` command would set the FTP port back to “21”.

- The following table lists the `ip service port` command options for specifying TCP/UDP services and also includes the default well-known port number associated with each service:

<table>
<thead>
<tr>
<th>service name</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>21</td>
</tr>
<tr>
<td>ssh</td>
<td>22</td>
</tr>
<tr>
<td>telnet</td>
<td>23</td>
</tr>
<tr>
<td>http</td>
<td>80</td>
</tr>
<tr>
<td>https</td>
<td>443</td>
</tr>
</tbody>
</table>

The `ntp` and `snmp` services are not supported with the `ip service port` command.
• Use the `ip service` command to enable or disable the status for a well-known or user-defined TCP/UDP service port.

**Examples**

-> ip service ftp port 20000  
-> ip service ftp port default  
-> ip service telnet port 20003  
-> ip service telnet port default

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- `ip service` Enables or disables well-known or user-defined service ports.
- `show ip service` Displays the IP service TCP/UDP port configuration and status.

**MIB Objects**

- `alaIpServiceTable`
  - `alaIpServiceType`
  - `alaIpServicePort`
  - `alaIpServiceStatus`
# ip service source-ip

Configures a user-defined source IP address as the outgoing IP interface for the IP service.

```
[vrf vrf_name] ip service source-ip {Loopback0 | interface_name} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
```

```
[vrf vrf_name] no ip service source-ip {Loopback0 | interface_name} [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
```

## Syntax Definitions

**vrf_name**
Name of the VRF.

**Loopback0**
Uses the Loopback0 interface as the source IP for the IP service.

**interface_name**
Specifies the name of the interface.

**tftp**
Configures the source IP address to be used by TFTP.

**telnet**
Configures the source IP address to be used by TELNET.

**tacacs**
Configures the source IP address to be used by TACACS.

**swlog**
Configures the source IP address to be used by SWLOG.

**ssh**
Configures the source IP address to be used by SSH.

**snmp**
Configures the source IP address to be used by SNMP.

**sflow**
Configures the source IP address to be used by sFlow. *This parameter is supported on both default VRF and non-default VRF instance.*

**radius**
Configures the source IP address to be used by RADIUS.

**ntp**
Configures the source IP address to be used by NTP.

**ldap**
Configures the source IP address to be used by the LDAP server.

**ftp**
Configures the source IP address to be used by FTP.

**dns**
Configures the source IP address to be used by DNS. *This parameter is supported only in the default VRF instance.*

**all**
Configures the source IP address to be used by all the applications.

## Defaults

By default, the outgoing interface is taken as the source IP address for all the applications.

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- If for a particular application, specific source IP address is configured and the “all” option is also set, the configured source IP address for the application is used as the outgoing interface.
- Use the **no** form of this command to revert to the default behavior.
- Configuring a source IP address for an IP service is supported in non-default VRF instances; however, the DNS feature is not supported in a non-default VRF, so only configure it in the default VRF.

**Examples**

```plaintext
-> ip service source-ip loopback0 telnet
-> ip service source-ip ipVlan100 ftp

-> vrf create vrf-1
vrf-1::-> ip service source-ip v-200 all
WARNING: SFLOW and DNS are not supported for non-default VRF, vrf-1
```

**Release History**

- Release 7.3.4; command introduced
- Release 8.5R4; **ntp** option deprecated.
- Release 8.6R2; **ntp** option re-introduced.
- Release 8.9R1; non-default VRF support for source-ip on sFlow added.

**Related Commands**

- `show ip service source-ip` Displays the IP service TCP/UDP port configuration and status.

**MIB Objects**

- `alaIpServiceSourceIPTable`  
  - `AlaIpServiceSourceIPAppIndex`  
  - `alaIpServiceSourceIPName`
### ip redist

Controls the conditions for redistributing IPv4 routes between different protocols.

```
[vrf vrf_name] ip redist [local | static | rip | ospf | isis | bgp | spb-mgmt | import] into {rip | ospf | isis | bgp | spb-mgmt} {all-routes | route-map route_map_name} [admin-state {enable | disable}]
```

```
no ip redist [local | static | rip | ospf | isis | bgp | spb-mgmt | import] into {rip | ospf | isis | bgp | spb-mgmt} {all-routes | route-map | route_map_name}
```

### Syntax Definitions

- **vrf_name**: The name of an existing VRF instance.
- **local**: Redistributes local routes.
- **static**: Redistributes static routes.
- **rip**: Specifies RIP as the source or destination (into) protocol.
- **ospf**: Specifies OSPF as the source or destination (into) protocol.
- **isis**: Specifies IS-IS as the source or destination (into) protocol.
- **bgp**: Specifies BGP as the source or destination (into) protocol.
- **spb-mgmt**: Specifies SPB management routes as the source or destination (into) protocol.
- **import**: Redistributes imported routes to other routing protocols.
- **all-routes**: Redistributes all routes. This option does not allocate route-map resources.
- **route_map_name**: Name of an existing route map that controls the redistribution of routes between the source and destination protocol.
- **enable**: Enables the administrative status of the redistribution configuration.
- **disable**: Disables the administrative status of the redistribution configuration.

### Defaults

If a VRF name is not specified with this command, routes are redistributed within the context of the active VRF instance.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the `no` form of this command to remove a route map redistribution configuration. If a route map name is not specified, all route maps associated with the redistribution configuration are removed.

- The source and destination protocols must be loaded and enabled before redistribution occurs.

- When configuring in-band management access to an SPB network domain:
  - Specify `spb-mgmt` as the source protocol to redistribute SPB management routes into dynamic routing protocols.
  - Specify `spb-mgmt` as the destination protocol to redistribute routes into ISIS-SPB.

- If the metric calculated for the redistributed route is greater than 15 (RIP_UNREACHABLE) or greater than the metric of an existing pure RIP route, the new route is not redistributed.

- Use the `ip route-map` commands described in this chapter to create a route map. Refer to the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.

Examples

```bash
-> ip redist rip into bgp route-map rip-to-bgp1
-> ip redist rip into bgp route-map rip-to-bgp2
-> no ip redist rip into bgp route-map rip-to-bgp2
-> ip redist ospf into rip route-map ospf-to-rip
-> ip redist ospf into rip route-map ospf-to-rip admin-state disable
-> ip redist import into ospf route-map R1 admin-state enable
-> ip redist spb-mgmt into ospf all-routes
-> ip redist ospf into spb-mgmt all-routes
```

Release History

Release 7.1.1; command introduced
Release 7.3.1; `vrf` and `import` parameters added.
Release 7.3.2; `all-routes` parameter added.
Release 8.7R2; `spb-mgmt` parameter added.

Related Commands

- `show ip redist` Displays the route map redistribution configuration.
- `ip route-map action` Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
- `ip import` Configures a route map to import routes from GRT to the destination VRF.
- `show ip import` Displays the import route configuration details.
**MIB Objects**

alaRouteMapRedistProtoTable
  alaRouteMapRedistSrcProtoId
  alaRouteMapRedistDestProtoId
  alaRouteMapRedistRouteMapIndex
  alaRouteMapRedistStatus
  alaRouteMapRedistAddressType
  alaRouteMapRedistRowStatus
ip access-list

Creates an access list for adding multiple IPv4 addresses to route maps.

ip access-list access_list_name
no ip access-list access_list_name

Syntax Definitions

access_list_name    Name of the access list (up to 20 characters).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release History</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the no form of this command to delete the access list.

Examples

-> ip access-list access1
-> no ip access-list access1

Release History

Release 7.1.1; command introduced

Related Commands

ip access-list address          Adds IPv4 addresses to the specified IPv4 access list.
show ip access-list            Displays the details of the access list.

MIB Objects

alaRouteMapAccessListNameTable
alaRouteMapAccessListName
alaRouteMapAccessListNameIndex
alaRouteMapAccessListNameAddressType
<table>
<thead>
<tr>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaRouteMapAccessListNameRowStatus</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ip access-list address

Adds multiple IPv4 addresses to the specified IPv4 access list.

```
ip access-list access_list_name address address/prefixLen [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
```

```
o ip access-list access_list_name address address/prefixLen
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>access_list_name</th>
<th>Name of the access list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>address/prefixLen</td>
<td>IP address/prefix length to be added to the access list.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits the IP address.</td>
</tr>
<tr>
<td>deny</td>
<td>Denies the IP address.</td>
</tr>
<tr>
<td>all-subnets</td>
<td>Permits or denies all the subnet routes that match the network portion of the IP address as specified by the mask length.</td>
</tr>
<tr>
<td>no-subnets</td>
<td>Permits or denies only those routes that exactly match the IP address and the mask length.</td>
</tr>
<tr>
<td>aggregate</td>
<td>Permits an aggregate route if there are one or more routes that match or are subnets of this address.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
<tr>
<td>all-subnets</td>
<td>no-subnets</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete the address from the access list.
- The **access_list_name** must exist before you add multiple addresses to the list.
- The **action** parameters (**permit** and **deny**) determine if a route that matches the **redist-control** configuration for the IP address is allowed or denied.
- The `redist-control` parameters (all-subnets, no-subnets, and aggregate) defines the criteria used to determine if a route matches an address in the access list.

- Configuring the combination of `redist-control aggregate` with `action deny` is not allowed.

- Use this command multiple times with the same access list name to add multiple addresses to the existing access list.

**Examples**

```plaintext
-> ip access-list access1 address 10.0.0.0/8 action permit
-> ip access-list access1 address 11.1.0.0/16 action permit
-> ip access-list access1 address 10.1.1.0/24 redist-control aggregate
-> no ip access-list access1 address 10.0.0.0/8
```

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **ip access-list**
  
  Creates an access list for adding multiple IPv4 addresses to route maps.

- **show ip access-list**
  
  Displays the contents of an IPv4 access list.

**MIB Objects**

- ```plaintext
  alaRouteMapAccessListTable
  alaRouteMapAccessListIndex
  alaRouteMapAccessListAddress
  alaRouteMapAccessListAddressType
  alaRouteMapAccessListPrefixLength
  alaRouteMapAccessListAction
  alaRouteMapAccessListRedistControl
  alaRouteMapAccessListRowStatus
```
**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

```
ip route-map route_map_name [sequence-number number] action {permit | deny}
no ip route-map route_map_name [sequence-number number]
```

---

**Syntax Definitions**

- `route_map_name`: The name of the route map (up to 20 characters).
- `number`: A number that links together the route maps. The range is 1–100.
- `permit`: Selects a route.
- `deny`: Filters a route.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>50</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>permit</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to delete the entire route map by specifying only the `route_map_name`.
- Use the `no` form of this command to delete a specific sequence in the route map by specifying the `sequence-number`.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- Use this command to change the status of an existing route map to permit or deny.

---

**Examples**

```
-> ip route-map route1 sequence-number 10 action permit
-> no ip route-map route1
```
**Release History**

Release 7.1.1; command introduced

**Related Commands**

**show ip route-map**

Displays the configured IP route maps.

**MIB Objects**

alaRouteMapSequenceTable
  alaRouteMapSequenceIndex
  alaRouteMapSequenceNumber
  alaRouteMapSequenceAction
  alaRouteMapSequenceRowStatus
**ip route-map match ip address**

Matches the route with the specified IPv4 address or an address defined in the specified IPv4 access list.

```
ip route-map route_map_name [sequence-number number] match ip-address {access_list_name | ip_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]}
```

```
no ip route-map route_map_name [sequence-number number] match ip-address {access_list_name | ip_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]}
```

---

**Syntax Definitions**

- `route_map_name`: The name of the route map.
- `number`: A number that links together the route maps. The range is 1–100.
- `access_list_name`: The name of an IPv4 access list that contains IPv4 addresses to match.
- `ip_address/prefixLen`: The destination IP address along with the prefix length of the routes to be selected.
- `all-subnets`: Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
- `no-subnets`: Selects only those routes that exactly match the IP address and the mask length.
- `aggregate`: Creates an aggregate route if there are one or more routes that match the IP address.
- `permit`: Permits a route based on the IP address or prefix constrained by redist-control.
- `deny`: Denies a route based on the IP address or prefix constrained by redist-control.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---
**Usage Guidelines**

- Use the no form of this command to delete the **match ip-address redist-control** parameter in the route map.

- Specify either the name of an existing IPv4 access list or an IPv4 address/prefix length with this command.

- Configuring the combination of **redist-control aggregate** with **deny** is not allowed.

- Multiple addresses in the same route map sequence are matched using the longest prefix match.

- If the best matching address is type **deny**, then the route is not selected. If the best matching address is type **permit** and the route map action is **deny**, the route is not selected.

- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.

- The **route_map_name**, **sequence-number**, and **access_list_name** (if used) must exist before you configure this **match** criteria.

**Examples**

```
-> ip route-map 3 match ip-address 10.1.1.1/8 redist-control no-subnets deny
-> no ip route-map 3 match ip-address 10.1.1.1 redist-control no-subnets deny
-> ip route-map routel sequence-number 10 match ip-address list1
-> no ip route-map routel sequence-number 10 match ip-address list1
```

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **ip route-map action**
  - Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **ip access-list**
  - Creates an access list for adding multiple IPv4 addresses to route maps.

- **ip access-list address**
  - Adds IPv4 addresses to the specified IPv4 access list.

- **show ip route-map**
  - Displays the configured IP route maps.

**MIB Objects**

- **alaRouteMapTable**
  - **alaRouteMapIndex**
  - **alaRouteMapSequence**
  - **alaRouteMapType**
  - **alaRouteMapValue**
  - **alaRouteMapRowStatus**
# ip route-map match ipv6 address

Matches the route with the specified IPv6 address or an address defined in the specified IPv6 access list.

```plaintext
ip route-map route_map_name [sequence-number number] match ipv6-address {access_list_name | ipv6_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]
```

```plaintext
no ip route-map route_map_name [sequence-number number] match ipv6-address ipv6_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}] [permit | deny]
```

## Syntax Definitions

- `route_map_name` - The name of the route map (up to 20 characters).
- `number` - A number that links together the route maps. The range is 1–100.
- `access_list_name` - The name of an IPv6 access list that contains IPv6 addresses to match.
- `ipv6_address/prefixLen` - The destination IPv6 address along with the prefix length of the routes to be selected.
- `all-subnets` - Selects all the subnet routes that match the network portion of the IP address as specified by the mask length.
- `no-subnets` - Selects only those routes that exactly match the IP address and the mask length.
- `aggregate` - Creates an aggregate route if there are one or more routes that match the IPv6 address.
- `permit` - Permits a route based on the IPv6 address or prefix constrained by redist-control.
- `deny` - Denies a route based on the IPv6 address or prefix constrained by redist-control.

## Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>50</td>
</tr>
<tr>
<td>`permit</td>
<td>deny`</td>
</tr>
</tbody>
</table>

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the no form of this command to delete the match ipv6-address redist-control parameter in the route map.
- Specify either the name of an existing IPv6 access list or an IPv6 address/prefix length with this command.
- Configuring the combination of redist-control aggregate with deny is not allowed.
- Multiple addresses in the same route map sequence are matched using the longest prefix match.
- If the best matching address is type deny, then the route is not selected. If the best matching address is type permit and the route map action is deny, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The route_map_name and sequence-number must exist before you configure this match criteria.

Examples

- ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
- no ip route-map 3 match ipv6-address 2001::1/64 redist-control no-subnets deny
- ip route-map route1 sequence-number 10 match ipv6-address list1
- no ip route-map route1 sequence-number 10 match ipv6-address list1

Release History

Release 7.1.1; command introduced

Related Commands

- ip route-map action
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- ipv6 access-list
  Creates an access list for adding multiple IPv6 addresses to route maps.

- ipv6 access-list address
  Adds IPv6 addresses to the specified IPv6 access list.

- show ip route-map
  Displays the configured IP route maps.

MIB Objects

alaRouteMapTable
  a1aRouteMapIndex
  a1aRouteMapSequence
  a1aRouteMapType
  a1aRouteMapValue
  a1aRouteMapRowStatus
**ip route-map match ip-nexthop**

Matches any routes that have a next-hop router address permitted by the specified access list name or the IP address specified in the route map.

```
ip route-map route_map_name [sequence-number number] match ip-nexthop {access_list_name | ip_address/prefixLen [permit | deny]}
```

```
no ip route-map route_map_name [sequence-number number] match ip-nexthop {access_list_name | ip_address/prefixLen [permit | deny]}
```

### Syntax Definitions

- **route_map_name**
  - The name of the route map.
- **number**
  - A number that links together the route maps. The range is 1–100.
- **access_list_name**
  - The access list that matches the route nexthop IP address.
- **ip_address/prefixLen**
  - The IP address along with the prefix length that matches any nexthop IP address within the specified subnet.
- **permit**
  - Permits a route based on the IP nexthop.
- **deny**
  - Denies a route based on the IP nexthop.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to delete the match ip-nexthop parameter in the route map.
- If the best matching nexthop is type deny, then the route is not selected. If the best matching nexthop is type permit and the route map action is deny, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The route_map_name, sequence-number, and access_list_name must exist before you configure this match criteria.
Examples

-> ip route-map route1 sequence-number 10 match ip-nexthop list1
-> no ip route-map route1 sequence-number 10 match ip-nexthop list1
-> ip route-map route1 sequence-number 10 match ip-nexthop 10.0.0.0/8
-> no ip route-map route1 sequence-number 10 match ip-nexthop 10.0.0.0/8

Release History

Release 7.1.1; command introduced

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list</td>
<td>Creates an access list for adding multiple IPv4 addresses to route maps.</td>
</tr>
<tr>
<td>ip access-list address</td>
<td>Adds IPv4 addresses to the specified IPv4 access list.</td>
</tr>
<tr>
<td>ip route-map action</td>
<td>Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.</td>
</tr>
<tr>
<td>show ip route-map</td>
<td>Displays the configured IP route maps.</td>
</tr>
</tbody>
</table>

MIB Objects

alaRouteMapTable
  alaRouteMapIndex
  alaRouteMapSequence
  alaRouteMapType
  alaRouteMapValue
  alaRouteMapRowStatus
**ip route-map match ipv6-nexthop**

Matches any routes that have an IPv6 next-hop router address permitted by the specified access list name or the IPv6 address specified in the route map.

```
ip route-map route_map_name [sequence-number number] match ipv6-nexthop {access_list_name | ipv6_address/prefixLen [permit | deny]}
no ip route-map route_map_name [sequence-number number] match ipv6-nexthop {access_list_name | ipv6_address/prefixLen [permit | deny]}
```

**Syntax Definitions**

- `route_map_name`: The name of the route map.
- `number`: A number that links together the route maps. The range is 1–100.
- `access_list_name`: The access list that matches the route nexthop IPv6 address.
- `ipv6_address/prefixLen`: The IPv6 address along with the prefix length that matches any nexthop IP address within the specified subnet.
- `permit`: Permits a route based on the IPv6 nexthop.
- `deny`: Denies a route based on the IPv6 nexthop.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete the **match ipv6-nexthop** parameter in the route map.
- If the best matching nexthop is type **deny**, then the route is not selected. If the best matching nexthop is type **permit** but the route map action is **deny**, the route is not selected.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The **route_map_name**, **sequence-number**, and **access_list_name** must exist before you configure this **match** criteria.
Examples

-> ip route-map route1 sequence-number 10 match ipv6-nexthop list1
-> no ip route-map route1 sequence-number 10 match ipv6-nexthop list1
-> ip route-map route1 sequence-number 10 match ipv6-nexthop 2001::/64
-> no ip route-map route1 sequence-number 10 match ipv6-nexthop 2001::/64

Release History

Release 7.1.1; command introduced

Related Commands

ipv6 access-list
 ipv6 access-list address
 ip route-map action
 show ip route-map

MIB Objects

alaRouteMapTable
  alaRouteMapIndex
  alaRouteMapSequence
  alaRouteMapType
  alaRouteMapValue
  alaRouteMapRowStatus
**ip route-map match tag**

Matches the tag value specified in the route map with the one on which the routing protocol learned the route.

```
ip route-map route_map_name [sequence-number number] match tag tag-number
no ip route-map route_map_name [sequence-number number] match tag tag_number
```

### Syntax Definitions

- **route_map_name**  
The name of the route map.
- **number**  
A number that links together the route maps. The range is 1–100.
- **tag_number**  
The tag number.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete the **match tag** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The **route_map_name** and **sequence-number** must exist before you configure this **match** criteria.

### Examples

```
-> ip route-map routel sequence-number 10 match tag 4
-> no ip route-map routel sequence-number 10 match tag 4
```

### Release History

Release 7.1.1; command introduced
**Related Commands**

- **ip route-map action**
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **show ip route-map**
  Displays the configured IP route maps.

**MIB Objects**

- `alaRouteMapTable`
  - `alaRouteMapIndex`
  - `alaRouteMapSequence`
  - `alaRouteMapType`
  - `alaRouteMapValue`
  - `alaRouteMapRowStatus`
**ip route-map match ipv4-interface**

Matches the IPv4 interface name specified in the route map with the interface on which the routing protocol learned the route.

```
ip route-map route_map_name [sequence-number number] match ipv4-interface interface_name
no ip route-map route_map_name [sequence-number number] match ipv4-interface interface_name
```

### Syntax Definitions

- **route_map_name**
  - The name of the route map.
- **number**
  - A number that links together the route maps. The range is 1–100.
- **interface_name**
  - Specifies the interface name of the outgoing interface of the route.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete the **match ipv4-interface** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The **route_map_name** and **sequence-number** must exist before you configure this **match** criteria.

### Examples

- `-> ip route-map route1 sequence-number 10 match ipv4-interface int4`
- `-> no ip route-map route1 sequence-number 10 match ipv4-interface int4`

### Release History

Release 7.1.1; command introduced
**Related Commands**

**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**show ip route-map**

Displays the configured IP route maps.

**MIB Objects**

alaRouteMapTable

- alaRouteMapIndex
- alaRouteMapSequence
- alaRouteMapType
- alaRouteMapValue
- alaRouteMapRowStatus
**ip route-map match ipv6-interface**

Matches the IPv6 interface name specified in the route map with the interface on which the routing protocol learned the route.

```
ip route-map route_map_name [sequence-number number] match ipv6-interface interface_name
no ip route-map route_map_name [sequence-number number] match ipv6-interface interface_name
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_map_name</td>
<td>The name of the route map.</td>
</tr>
<tr>
<td>number</td>
<td>A number that links together the route maps. The range is 1–100.</td>
</tr>
<tr>
<td>interface_name</td>
<td>Specifies the interface name of the outgoing interface of the route.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete the **match ipv6-interface** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The **route_map_name** and **sequence-number** must exist before you configure this **match** criteria.

**Examples**

- `-> ip route-map routel sequence-number 10 match ipv6-interface int6`
- `-> no ip route-map routel sequence-number 10 match ipv6-interface int6`

**Release History**

Release 7.1.1; command introduced
Related Commands

**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**show ip route-map**

Displays the configured IP route maps.

MIB Objects

```plaintext
alaRouteMapTable
  alaRouteMapIndex
  alaRouteMapSequence
  alaRouteMapType
  alaRouteMapValue
  alaRouteMapRowStatus
```
**ip route-map match metric**

Matches the metric value specified in the route map with the actual metric value of the route.

```
ip route-map route_map_name [sequence-number number] match metric metric [deviation deviation]
no ip route-map route_map_name [sequence-number number] match metric metric [deviation deviation]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_map_name</td>
<td>The name of the route map.</td>
</tr>
<tr>
<td>number</td>
<td>A number that links together the route maps. The range is 1–100.</td>
</tr>
<tr>
<td>metric</td>
<td>The metric value that matches a specified metric.</td>
</tr>
<tr>
<td>deviation</td>
<td>The deviation value. If deviation is included, the route metric can have any value within the range (metric-deviation to metric+deviation).</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to delete the `match metric` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `match` criteria.

### Examples

```
-> ip route-map route1 sequence-number 10 match metric 4
-> no ip route-map route1 sequence-number 10 match metric 4
```

### Release History

Release 7.1.1; command introduced
**Related Commands**

**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**show ip route-map**

Displays the configured IP route maps.

**MIB Objects**

alaRouteMapTable
  - alaRouteMapIndex
  - alaRouteMapSequence
  - alaRouteMapType
  - alaRouteMapValue
  - alaRouteMapRowStatus
ip route-map match route-type

Matches the specified route type with actual route type of the route.

```
ip route-map route_map_name [sequence-number number] match route-type {internal | external [type1 | type2] | level1 | level2}
no ip route-map route_map_name [sequence-number number] match route-type {internal | external [type1 | type2] | level1 | level2}
```

### Syntax Definitions

- **route_map_name**: The name of the route map.
- **number**: A number that links together the route maps. The range is 1–100.
- **internal**: Matches OSPF/BGP internal routes.
- **external**: Matches OSPF/BGP external routes.
- **type1**: Matches OSPF external Type-1 routes, which gives the full metric calculation for the complete path including internal as well as external cost.
- **type2**: Matches OSPF external Type-2 routes, which gives the external redistribution metric only to the ASBR.
- **level1**: Matches IS-IS Level-1 routes only.
- **level2**: Matches IS-IS Level-2 routes only.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete the **match route-type** parameter in the route map.

- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.

- The **route_map_name** and **sequence-number** must exist before you configure this **match** criteria.
**Examples**

-> ip route-map 111 sequence-number 50 match route-type internal
-> no ip route-map 111 sequence-number 50 match route-type internal

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- `ip route-map action` Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
- `show ip route-map` Displays the configured IP route maps.

**MIB Objects**

`alaRouteMapTable`
  - `alaRouteMapIndex`
  - `alaRouteMapSequence`
  - `alaRouteMapType`
  - `alaRouteMapValue`
  - `alaRouteMapRowStatus`
**ip route-map match protocol**

Matches the protocol specified in the route map with the protocol of the route.

```
ip route-map route_map_name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp}
no ip route-map route_map_name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp}
```

### Syntax Definitions

- `route_map_name`: The name of the route map.
- `number`: A number that links together the route maps. The range is 1–100.
- `local`: Matches a local interface route.
- `static`: Matches a static route.
- `rip`: Matches a RIP route.
- `ospf`: Matches an OSPF route.
- `isis`: Matches an IS-IS route.
- `bgp`: Matches a BGP route.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>number</code></td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8</th>
<th>C32E/T24C2</th>
<th>X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to delete the `match protocol` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `match` criteria.

### Examples

```
-> ip route-map route1 sequence-number 10 match protocol local
```
-> no ip route-map route1 sequence-number 10 match protocol local

**Release History**

Release 7.3.1; command introduced

**Related Commands**

- **ip route-map action**
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **show ip route-map**
  Displays the configured IP route maps.

**MIB Objects**

alaRouteMapTable
  - alaRouteMapIndex
  - alaRouteMapSequence
  - alaRouteMapType
  - alaRouteMapValue
  - alaRouteMapRowStatus
**ip route-map match name**

Matches the name of a static route specified in the route map with the name of the static route.

```
ip route-map route_map_name [sequence-number number] match name string
no ip route-map route_map_name [sequence-number number] match name string
```

### Syntax Definitions

- `route_map_name` The name of the route map.
- `number` A number that links together the route maps. The range is 1–100.
- `name string` The name of the static route to match.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete the `match name` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `match` criteria.

### Examples

- `-> ip route-map routel sequence-number 10 match name Route-Bldgl`
- `-> no ip route-map routel sequence-number 10 match name Route-Bldgl`

### Release History

Release 7.3.1; command introduced
### Related Commands

**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**show ip route-map**

Displays the configured IP route maps.

### MIB Objects

<table>
<thead>
<tr>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaRouteMapTable</td>
</tr>
<tr>
<td>alaRouteMapIndex</td>
</tr>
<tr>
<td>alaRouteMapSequence</td>
</tr>
<tr>
<td>alaRouteMapType</td>
</tr>
<tr>
<td>alaRouteMapValue</td>
</tr>
<tr>
<td>alaRouteMapRowStatus</td>
</tr>
</tbody>
</table>
ip route-map set metric

Configures the metric value of the route being distributed.

```
ip route-map route_map_name [sequence-number number] set metric metric [effect {add | subtract | replace | none}]
no ip route-map route_map_name [sequence-number number] set metric metric [effect {add | subtract | replace | none}]
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_map_name</td>
<td>The name of the route map.</td>
</tr>
<tr>
<td>number</td>
<td>A number that links together the route maps. The range is 1–100.</td>
</tr>
<tr>
<td>metric</td>
<td>Configures the metric value of the route. A value of 0 is not allowed.</td>
</tr>
<tr>
<td>add</td>
<td>Adds the configured metric value to the actual metric value.</td>
</tr>
<tr>
<td>subtract</td>
<td>Subtracts the configured metric value from the actual metric value.</td>
</tr>
<tr>
<td>replace</td>
<td>Replaces the actual metric value with the configured metric value.</td>
</tr>
<tr>
<td>none</td>
<td>Uses the actual metric value of the route. The configured metric value is ignored. Use any value except 0.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the `set metric` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `set` criteria.

**Examples**

```
-> ip route-map 111 sequence-number 50 set metric 30 effect add
-> no ip route-map 111 sequence-number 50 set metric 30 effect add
```
**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **ip route-map action**
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **show ip route-map**
  Displays the configured IP route maps.

**MIB Objects**

alaRouteMapTable
  - alaRouteMapIndex
  - alaRouteMapSequence
  - alaRouteMapType
  - alaRouteMapValue
  - alaRouteMapRowStatus
**ip route-map set metric-type**

Configures the metric type for the redistributed route.

```
ip route-map route_map_name [sequence-number number] set metric-type {internal | external [type1 | type2]}
no ip route-map route_map_name [sequence-number number] set metric-type {internal | external [type1 | type2]}
```

**Syntax Definitions**

- **route_map_name**: The name of the route map.
- **number**: A number that links together the route maps. The range is 1–100.
- **internal**: Sets the metric type to internal for routes redistributed into BGP.
- **external**: Sets the metric type to external for routes redistributed into BGP.
- **type1**: Sets the metric type to external type1 for routes redistributed into OSPF, which gives the full metric calculation for the complete path including internal as well as external cost.
- **type2**: Sets the metric type to external type2 for routes redistributed into OSPF, which gives the external redistribution metric only to the ASBR.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete the **set metric-type** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The **route_map_name** and **sequence-number** must exist before you configure this **set** criteria.

**Examples**

```
-> ip route-map 111 sequence-number 50 set metric-type internal
```
-> no ip route-map 111 sequence-number 50 set metric-type internal

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **ip route-map action**
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **show ip route-map**
  Displays the configured IP route maps.

**MIB Objects**

alaRouteMapTable
  - alaRouteMapIndex
  - alaRouteMapSequence
  - alaRouteMapType
  - alaRouteMapValue
  - alaRouteMapRowStatus
**ip route-map set tag**

Configures the tag value of the selected routes.

```plaintext
ip route-map route_map_name [sequence-number number] set tag tag_number
no ip route-map route_map_name [sequence-number number] set tag tag_number
```

### Syntax Definitions

- **route_map_name**: The name of the route map.
- **number**: A number that links together the route maps. The range is 1–100.
- **tag_number**: Configures the tag number.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>release</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete the **set tag** parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The **route_map_name** and **sequence-number** must exist before you configure this **set** criteria.

### Examples

- `-> ip route-map 111 sequence-number 50 set tag 23`
- `-> no ip route-map 111 sequence-number 50 set tag 23`

### Release History

Release 7.1.1; command introduced
Related Commands

**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**show ip route-map**

Displays the configured IP route maps.

MIB Objects

alaRouteMapTable

- alaRouteMapIndex
- alaRouteMapSequence
- alaRouteMapType
- alaRouteMapValue
- alaRouteMapRowStatus
**ip route-map set community**

Configures the community name of the route being redistributed into BGP.

```
ip route-map route_map_name [sequence-number number] set community community_string
no ip route-map route_map_name [sequence-number number] set community community_string
```

**Syntax Definitions**

- `route_map_name`: The name of the route map.
- `number`: A number that links together the route maps. The range is 1–100.
- `community_string`: Defines a community for an aggregate route. Community names range from 0 to 70 characters.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the `set community` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `set` criteria.

**Examples**

```
-> ip route-map 111 sequence-number 50 set community 29
-> no ip route-map 111 sequence-number 50 set community 29
```

**Release History**

Release 7.1.1; command introduced
**Related Commands**

`ip route-map action`  
Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

`show ip route-map`  
Displays the configured IP route maps.

**MIB Objects**

`alaRouteMapTable`  
- `alaRouteMapIndex`
- `alaRouteMapSequence`
- `alaRouteMapType`
- `alaRouteMapValue`
- `alaRouteMapRowStatus`
ip route-map set local-preference

Configures the local preference value for a route being distributed into BGP.

```
ip route-map route_map_name [sequence-number number] set local-preference value
no ip route-map route_map_name [sequence-number number] set local-preference value
```

**Syntax Definitions**

- `route_map_name`: The name of the route map.
- `number`: A number that links together the route maps. The range is 1–100.
- `value`: Configures the local-preference value for routes being redistributed in to BGP. The value is between 0 and 4294967295.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the `set local-preference` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `set` criteria.
- The local preference attribute is used to set preference to an exit point from the local autonomous system (AS).
- If there are multiple exit points from the AS, the local preference attribute is used to select the exit point for a specific route.

**Examples**

```
-> ip route-map 111 sequence-number 50 set local-preference 4
-> no ip route-map 111 sequence-number 50 set local-preference 4
```
**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **ip route-map action**
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **show ip route-map**
  Displays the configured IP route maps.

**MIB Objects**

alaRouteMapTable
- alaRouteMapIndex
- alaRouteMapSequence
- alaRouteMapType
- alaRouteMapValue
- alaRouteMapRowStatus
ip route-map set level

Configures the level of the selected ISIS route.

```
ip route-map route_map_name [sequence-number number] set level {level1 | level2 | level1-2}
no ip route-map route_map_name [sequence-number number] set level {level1 | level2 | level1-2}
```

**Syntax Definitions**

- `route_map_name`: The name of the route map.
- `number`: A number that links together the route maps. The range is 1–100.
- `level1`: Matches IS-IS Level-1 routes only.
- `level2`: Matches IS-IS Level-2 routes only.
- `level1-2`: Matches IS-IS Level1-2 routes.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the `set level` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `set` criteria.

**Examples**

```
-> ip route-map 111 sequence-number 50 set level level1
-> no ip route-map 111 sequence-number 50 set level level1
```

**Release History**

Release 7.1.1; command introduced
**Related Commands**

- **ip route-map action**
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **show ip route-map**
  Displays the configured IP route maps.

**MIB Objects**

- `alaRouteMapTable`
  - `alaRouteMapIndex`
  - `alaRouteMapSequence`
  - `alaRouteMapType`
  - `alaRouteMapValue`
  - `alaRouteMapRowStatus`
**ip route-map set ip-nexthop**

Configures the IP address of the next hop in a route map.

```
ip route-map route_map_name [sequence-number number] set ip-nexthop ip_address
no ip route-map route_map_name [sequence-number number] set ip-nexthop ip_address
```

### Syntax Definitions

- **route_map_name**: The name of the route map.
- **number**: A number that links together the route maps. The range is 1–100.
- **ip_address**: IP address of the next hop.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>50</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to delete the set ip-nexthop parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The route_map_name and sequence-number must exist before you configure this set criteria.

### Examples

```
-> ip route-map 222 sequence-number 50 set ip-nexthop 128.251.17.224
-> no ip route-map 222 sequence-number 50 set ip-nexthop 128.251.17.224
```

### Release History

Release 7.1.1; command introduced
Related Commands

**ip route-map action**
Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**show ip route-map**
Displays the configured IP route maps.

MIB Objects

alaIPRouteMapTable
alaRouteMapIndex
alaRouteMapSequence
alaRouteMapType
alaRouteMapValue
alaRouteMapRowStatus
ip route-map set ipv6-nexthop

Configures the IPv6 address of the next hop in a route map.

`ip route-map route_map_name [sequence-number number] set ipv6-nexthop ipv6_address`

`no ip route-map route_map_name [sequence-number number] set ipv6-nexthop ipv6_address`

**Syntax Definitions**

- `route_map_name` The name of the route map.
- `number` A number that links together the route maps. The range is 1–100.
- `ipv6_address` IPv6 address of the next hop.

**Defaults**

- `number` default 50

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the `set ipv6-nexthop` parameter in the route map.
- All route maps having the same name but different sequence numbers are linked together and processed in order of increasing sequence number.
- The `route_map_name` and `sequence-number` must exist before you configure this `set` criteria.

**Examples**

- `-> ip route-map 222 sequence-number 50 set ipv6-nexthop 2001::1`
- `-> no ip route-map 222 sequence-number 50 set ipv6-nexthop 2001::1`

**Release History**

Release 7.1.1; command introduced
Related Commands

**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**show ip route-map**

Displays the configured IP route maps.

MIB Objects

alaIPRouteMapTable
  alaRouteMapIndex
  alaRouteMapSequence
  alaRouteMapType
  alaRouteMapValue
  alaRouteMapRowStatus
vrf

Configures and selects a virtual routing and forwarding (VRF) instance on the switch.

vrf [create] [vrf_name | default] [profile {max | low}]
no vrf vrf_name

Syntax Definitions

create
Creates a new VRF instance with the specified VRF name.

vrf_name
The alphanumeric name (1–20 characters) assigned to the VRF instance.

default
Optional. Selects the default VRF instance.

max
Creates a VRF with the maximum profile capabilities.

low
Creates a VRF with the minimum (lowest) capabilities. Low profile VRFs use less system resources.

Defaults

A default VRF instance exists in the switch configuration. All applications that are not VRF aware belong to this instance.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf_name</td>
<td>default VRF instance</td>
</tr>
<tr>
<td>max</td>
<td>max profile</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- To create a new VRF instance, use the create parameter with this command. For example, vrf create IpOne creates a new “IpOne” VRF instance. When a new instance is created, that instance automatically becomes the current CLI context.

- If the create keyword is not specified, then this command will select the specified VRF name as the current CLI context. If the VRF instance does not exist, an error message is displayed.

- Use the no form of this command to delete a VRF instance. Deleting the default instance is not allowed. In addition, any interfaces configured for a VRF instance are automatically removed when the instance is deleted.
• To return to the default VRF instance from within the context of another instance, enter the `vrf` command with or without the optional `default` parameter (for example, `vrf` or `vrf default`).

• Configuring a VRF instance name is case sensitive. Use the `show vrf` command to verify the VRF instance configuration before selecting, adding, or removing instances.

• If the name of an existing instance is specified with this command, VRF changes the command prompt to reflect the specified instance name. All CLI commands entered at this point are applied within the context of the active VRF instance.

• It is also possible to configure other instances from within the CLI context of the default VRF instance by entering the `vrf` command followed by the instance name. For example, entering `vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100` is applied to the IpOne instance even though IpOne is not the active CLI context.

• The type of profile assigned to a VRF instance determines the routing protocols and capabilities supported within that instance. For example:
  – Low profile VRFs only support IPv4 and VRRP with routing capabilities restricted to static and imported routes. In addition, limiting low profiles to 9 routes and 3 IP interfaces is highly recommended.
  – IPv6 routing protocols (such as BGP, IS-IS, PIM, RIPng, OSPFv3, and VRRPv3) are only supported on max profile VRFs.

• Profiles are not configurable for the default VRF, which provides full routing capabilities.

• Changing the profile for an existing VRF instance is not allowed. To change the profile, first delete the VRF then create it again with a different profile.

**Examples**

The following command examples create new VRF instances:

```
-> vrf create IpOne
IpOne:: ->
```

```
IpOne:: -> vrf create IpTwo
IpTwo:: ->
```

```
-> vrf create IpThree profile low
IpThree::->
```

The following command examples select a VRF instance to change the CLI context:

```
-> vrf IpTwo
IpTwo:: ->
```

```
-> vrf IpFour
ERROR: VRF IpFour does not exist.
```

The following command examples return the CLI context to the default VRF instance:

```
IpTwo:: -> vrf
->
```

```
IpTwo:: -> vrf default
->
```

The following command example configures an IP interface for the “IpOne” VRF instance from within the context of the default VRF instance:

```
-> vrf IpOne ip interface intf100 address 100.1.1.1/24 vlan 100
```
Release History

Release 7.1.1; command was introduced.
Release 7.3.2; max and low parameters added to define VRF profiles.
Release 8.4.1.R03; create parameter added.

Related Commands

- **show vrf**
  Displays the VRF instance configuration for the switch.
- **show vrf-profiles**
  Displays the VRF profile resources for the switch.
- **ip export**
  Exports VRF routes to the Global Routing Table (GRT).
- **ip import**
  Imports VRF routes from the GRT.

MIB Objects

alaVirtualRouterNameTable
  - alaVirtualRouterName
  - alaVirtualRouterNameIndex
  - alaVirtualRouterNameRowStatus
  - alaVirtualRouterProfile
### ip export

Exports routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances. All routes are exported or a route map can be specified to filter exported routes

```
[vrf vrf_name] ip export {all-routes | route-map route_map_name} to-all-vrfs {all-routes | route-map route_map_name}
```

```
[vrf vrf_name] no ip export
```

#### Syntax Definitions

- **vrf_name**
  - The name of an existing VRF instance. Routes are exported from this source VRF to the GRT.

- **all-routes**
  - Exports all routes from the source VRF to the GRT. This option does not allocate route-map resources.

- **route_map_name**
  - The name of an existing route-map to use for filtering routes that are exported from the source VRF to the GRT.

- **to-all-vrfs all-routes**
  - Exports all routes to all of the other VRF instances, except to VRFs that already have an import configured for the source (export) VRF.

- **to-all-vrfs route-map route_map_name**
  - The name of an existing route map to use for filtering routes that are exported from the source VRF to all other VRF instances.

#### Defaults

- If a source VRF name is not specified with this command, routes are exported from within the context of the active VRF instance to the GRT.

- If there are no VRF instances configured on the switch, the routes are exported from the default VRF to the GRT.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- Use the `no` form of this command to disable exporting of routes from the VRF to GRT.

- The route map name specified with this command must already exist in the switch configuration. See the `ip route-map` commands in this guide and the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.
A route map created to filter exported VRF routes can contain any of the following match and set options:
- Match options: ip-address, ip-next-hop, tag, protocol, ipv4-interface, metric, route-type, name
- Set options: tag, metric
A route map with redist control of aggregate is supported when exporting IP routes, but it is not supported when importing IP routes.
Only one route map per source VRF or ISID is allowed for filtering exported routes.
Only those FDB (Forwarding Routing Database) routes that match the conditions of the route map are exported to GRT.
Modifying a route map that is assigned to a VRF or ISID through the `ip import` or `ip export` command is supported.

**Examples**
The following commands export routes from the current VRF routing table (or from the default VRF if there are no other VRFs configured) to the GRT:

```bash
-> ip export route-map R1
-> ip export all-routes
-> ip export to-all-vrfs all-routes
-> ip export to-all-vrfs route-map R2
-> no ip export
```

The following commands export routes from the “vrf2” routing table to the GRT even though the command line is operating within the context of the default VRF instance:

```bash
-> vrf vrf2 ip export route-map R1
-> vrf vrf2 ip export all-routes
-> vrf vrf2 ip export to-all-vrfs all-routes
-> vrf vrf2 ip export to-all-vrfs route-map R2
-> no vrf vrf2 ip export
```

The following commands first change the command line context to the “vrf1” instance so that all subsequent commands export routes from “vrf1” without having to specify the VRF name with each command:

```bash
-> vrf vrf1
vrf1::-> ip export route-map R1
vrf1::-> ip export all-routes
vrf1::-> ip export to-all-vrfs all-routes
vrf1::-> ip export to-all-vrfs route-map R2
vrf1::-> no ip export
```

**Release History**
Release 7.3.1; command introduced.
Release 7.3.2; `all-routes` and `to-all-vrfs` parameters added.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vrf</strong></td>
<td>Configures and selects a virtual routing and forwarding (VRF) instance on the switch.</td>
</tr>
<tr>
<td><strong>ip route-map action</strong></td>
<td>Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.</td>
</tr>
<tr>
<td><strong>ip route-map match protocol</strong></td>
<td>Matches the protocol specified in the route map with the protocol of the route.</td>
</tr>
<tr>
<td><strong>show ip export</strong></td>
<td>Displays the export route configuration details.</td>
</tr>
<tr>
<td><strong>show ip global-route-table</strong></td>
<td>Displays the GRT for all the routes that are exported from the VRFs.</td>
</tr>
<tr>
<td><strong>show ip route-map</strong></td>
<td>Displays the configured IP route maps.</td>
</tr>
</tbody>
</table>

### MIB Objects

- alaIprmExportRouteMap
- alaIprmExportToAllVrfsRouteMap
ip import

Imports VRF or Shortest Path Bridging (SPB) service instance identifier (ISID) routes from the GRT to the destination VRF. All routes are imported or a route map can be specified to filter imported routes.

```plaintext
[vrf dest_vrf_name] ip import {vrf {src_vrf_name | default} | isid instance_id} {all-routes | route-map route_map_name}
```

```plaintext
[vrf dest_vrf_name] no ip import {vrf {src_vrf_name | default} | isid instance_id}
```

### Syntax Definitions

- **dest_vrf_name**
  The name of the destination VRF instance into which routes are imported from the GRT.

- **src_vrf_name**
  The name of the source VRF instance from which routes were exported to the GRT. Routes from this instance are imported from the GRT into the specified destination VRF instance.

- **default**
  Default VRF. The routes are imported from the default VRF instance.

- **instance_id**
  An existing ISID number that identifies an SPB service in a provider backbone bridge (PBB) network. The routes for this ISID number are imported from the GRT into the current or specified VRF instance.

- **all-routes**
  Imports all routes from the source VRF instance. Imported routes are not filtered.

- **route_map_name**
  The name of an existing route map to use for filtering routes that are imported from the GRT to the destination VRF. Imported routes are filtered based on the options defined in the route map.

### Defaults

If a destination VRF name is not specified with this command, routes are imported from the GRT into the context of the active VRF instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the IP import routes configuration for the specified VRF instance or ISID.

- The route map name specified with this command must already exist in the switch configuration. See the **ip route-map** commands in this guide and the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.
A route map created to filter imported VRF or ISID routes can contain any of the following match and set parameter options:
- Match options: ip-address, ip-next-hop, tag, metric
- Set options: tag, metric

A route map with redist control of aggregate is supported when exporting IP routes, but it is not supported when importing IP routes.

Only one route map per source (imported) VRF or ISID is allowed.

Modifying a route map that is assigned to a VRF or ISID through the `ip import` or `ip export` command is supported.

Leaked routes are only for forwarding. If a local route is leaked, that interface is not accessible in the importing VRF. Another switch will not be able to ping the interface in the import VRF.

**Examples**

-> ip import vrf V1 route-map R2
-> ip import vrf V2 all-routes
-> ip import isid 1500 route-map R1
-> ip import isid 2000 all-routes
-> no ip import vrf V1
-> no ip import isid 1500

**Release History**

Release 7.3.1; command introduced.
Release 7.3.2; `isid` and `all-routes` parameters added.

**Related Commands**

- `vrf` Configures and selects a virtual routing and forwarding (VRF) instance on the switch.
- `ip route-map action` Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
- `ip route-map match protocol` Matches the protocol specified in the route map with the protocol of the route.
- `show ip import` Displays the import route configuration details.
- `show ip global-route-table` Displays the GRT for all the routes that are exported from the VRFs.
- `show ip route-map` Displays the configured IP route maps.
MIB Objects

alaIprmImportVrfTable
  alaIprmImportVrfName
  alaIprmImportVrfRouteMap
  alaIprmImportVrfRowStatus
alaIprmImportIsidTable
  alaIprmImportIsid
  alaIprmImportIsidRouteMap
  alaIprmImportIsidRowStatus
**show ip export**

Displays the export route configuration details.

```
[vrf vrf_name] show ip export
```

### Syntax Definitions

- **vrf_name**  
The name of an existing VRF instance.

### Defaults

By default, the export route configuration for the active VRF instance is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If a VRF is specified, the export route configuration for that VRF is displayed.

### Examples

```
-> show ip export  
Export Route Map: leak-out

-> vrf vrf1 show ip export  
Export Route Map: none (all-routes)

vrf2:-> show ip export  
Export Route Map: none (all-routes) -> To All VRFs
```

### Release History

Release 7.3.1; command introduced.
Related Commands

ip export
Exports routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances.

MIB Objects

alaIprmExportRouteMap
alaIprmExportToAllVrfsRouteMap
show ip import

Displays the import route configuration details.

[vrf vrf_name] show ip import

Syntax Definitions

vrf_name The name of an existing VRF instance.

Defaults

By default, the import route configuration for the active VRF instance is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If a VRF is specified, the import route configuration for that VRF is displayed.

Examples

-> show ip import

<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
<th>RouteMap</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Customer1</td>
<td>leak-in</td>
</tr>
<tr>
<td>vrf</td>
<td>Customer2</td>
<td>none (all-routes)</td>
</tr>
<tr>
<td>isid</td>
<td>1000</td>
<td>isid1000-filter</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Type</th>
<th>The type of imported route (vrf or isid).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The name of the VRF instance or the Shortest Path Bridging service instance identifier (ISID) from which routes are imported to the VRF.</td>
</tr>
<tr>
<td>RouteMap</td>
<td>The name of the route map filter or none (all-routes).</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command introduced.
Release 7.3.2; VRF Name and Description fields renamed Type and Source, imported ISID route entries added to the table.
**Related Commands**

**ip import** Imports VRF or Shortest Path Bridging ISID routes from the GRT to the destination VRF.

**MIB Objects**

- `alaIprmImportVrfTable`
  - `alaIprmImportVrfName`
  - `alaIprmImportVrfRouteMap`
  - `alaIprmImportVrfRowStatus`
- `alaIprmImportIsidTable`
  - `alaIprmImportIsid`
  - `alaIprmImportIsidRouteMap`
  - `alaIprmImportIsidRowStatus`
show ip global-route-table

Displays the contents of the Global Routing Table (GRT) for all the routes that are exported from VRF instances or from Shortest Path Bridging service instance identifiers (ISIDs). This command is only available within the context of the default VRF instance.

show ip global-route-table [export-vrf vrf_name]

Syntax Definitions

vrf_name

The alphanumeric name (1–20 characters) assigned to the VRF instance.

Defaults

By default, exported routes are displayed for all VRF instances and ISIDs.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the export-vrf parameter to display exported routes for a specific VRF instance.

Examples

```
-> show ip global-route-table
Type  Source               Destination        Gateway         Metric  Tag
-----+--------------------+------------------+---------------+----------+----------
vrf  Customer1         10.0.0.0/8        12.1.1.2        1         100
vrf  Customer2         11.0.0.0/8        12.1.1.3        2         0
isid 1000              12.0.0.0/8        12.1.1.4        1         2
```

output definitions

<table>
<thead>
<tr>
<th>Type</th>
<th>The type of exported route (vrf or isid).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The name of the VRF instance or the Shortest Path Bridging service instance identifier (ISID) from which routes are exported to the GRT.</td>
</tr>
<tr>
<td>Destination</td>
<td>The address of the route.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The next hop for the destination address.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric of the exported route.</td>
</tr>
<tr>
<td>Tag</td>
<td>The tag of the exported route.</td>
</tr>
</tbody>
</table>
Release History

Release 7.3.1; command introduced.
Release 7.3.2; VRF Name and Description fields renamed Type and Source, exported ISID route entries added to the table.

Related Commands

**ip export**
Configures a route map to export routes from the source VRF to Global Routing Table (GRT).

**show ip export**
Displays the export route configuration details.

MIB Objects

alaGrtRouteTable
  alaGrtRouteDistinguisher
  alaGrtRouteDest
  alaGrtRouteMaskLen
  alaGrtRouteNextHop
  alaGrtRouteMetric
  alaGrtRouteTag
  alaGrtRouteVrfName
  alaGrtRouteIsid
arp

Adds a permanent entry to the ARP table. To forward packets, the switch dynamically builds an ARP Table to match the IP address of a device with its physical (MAC) address. These entries age out of the table when the timeout value is exceeded. This command is used to add a permanent entry to the table. Permanent entries do not age out of the table.

```
arp ip_address mac_address [alias] [name] [interface interface_name] [port chassis/slot/port] [linkagg agg_id]
```

```
no arp ip_address [alias]
```

**Syntax Definitions**

- **ip_address**  
  IP address of the device you are adding to the ARP table.

- **mac_address**  
  MAC address of the device in hexadecimal format (for example, 00.00.39.59.f1.0c).

- **alias**  
  Specifies that the switch will act as an alias (or proxy) for this IP address. When the alias option is used, the switch responds to all ARP requests for the specified IP address with its own MAC address. *This parameter is not supported on the OmniSwitch 9900.*

  The proxy feature can also be enabled for an IP interface using the **ip interface** command. When enabled, ARP requests return the MAC address of the IP router interface and all traffic within the VLAN is routed.

- **name**  
  The name to assign to this ARP entry.

- **interface_name**  
  Name of the interface to be used for ARP resolution.

- **chassis/slot/port**  
  The chassis ID, slot, and port number (1/1/3).

- **agg_id**  
  The link aggregate ID number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete a permanent ARP entry.
• Configuring a permanent ARP entry with a multicast address is also supported. This is done by specifying a multicast address for the \texttt{ip-address} parameter instead of a unicast address.

• Using the \texttt{arp alias} command is not related to proxy ARP as defined in RFC 925. Instead, \texttt{arp alias} is similar to the Local Proxy ARP feature, except that it is used to configure the switch as a proxy for only one IP address.

• As most hosts support the use of address resolution protocols to determine cache address information (called dynamic address resolution), it is not required to specify permanent ARP cache entries.

• Only the IP address is required when deleting an ARP entry from the table.

\textbf{Examples}

\begin{verbatim}
-> arp 171.11.1.1 00:05:02:c0:7f:11
-> arp 171.11.1.1 00:05:02:c0:7f:11 interface int1
-> no arp 171.11.1.1
\end{verbatim}

\textbf{Release History}

Release 7.1.1; command was introduced.
Release 7.3.4; \texttt{interface} parameter added.

\textbf{Related Commands}

\begin{verbatim}
\texttt{clear arp-cache} \hspace{1cm} Deletes all dynamic entries from the ARP table.
\texttt{ip interface} \hspace{1cm} Enables or disables the Local Proxy ARP feature for an IP interface. When enabled, all traffic within the VLAN is routed. ARP requests return the MAC address of the IP router interface.
\texttt{show arp} \hspace{1cm} Displays the ARP table.
\end{verbatim}

\textbf{MIB Objects}

\begin{verbatim}
\texttt{ipNetToMediaTable}
  ipNetToMediaIfIndex
  ipNetToMediaNetAddress
  ipNetToMediaPhyAddress
  ipNetToMediaType
\texttt{alaIpNetToMediaTable}
  alaIpNetToMediaPhyAddress
  alaIpNetToMediaProxy
\end{verbatim}
ip distributed-arp admin-state

Enables or disables the distributed ARP feature.

`ip distributed-arp admin-state {enable | disable}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Dynamically assigns a Network Interface (NI) as the designated-NI for all the ARP entries on an IP interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the distributed ARP feature.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- Use this feature to dynamically assign a Network Interface (NI) as the designated-NI for all the ARP entries. The NI with maximum number of active ports for that IP subnet is assigned.
- To reset or update the dynamically assigned NI, the feature must be disabled and then enabled.

**Examples**

-> ip distributed-arp admin-state enable
-> ip distributed-arp admin-state disable

**Release History**

Release 7.3.4; command introduced;
Release 8.6R2; command deprecated.

**Related Commands**

- `show ip arp utilization` Displays the designated NIs for the interfaces and the NI utilization.
- `show ip interface` Displays the configuration and status of IP interfaces.

**MIB Objects**

- `alaIpDistributedArp`
arp send-gratuitous-arp

Enables or disables the outgoing Gratuitous ARP packets.

`arp send-gratuitous-arp {enable | disable}`

**Syntax Definitions**

- **enable**: The Gratuitous ARP packets are periodically sent from the switch.
- **disable**: The outgoing Gratuitous ARP packets are blocked.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this feature to block the outgoing Gratuitous ARP packets from the switch.
- The incoming Gratuitous ARP packets can be blocked or allowed using the `ip dos type` CLI command.
- The configuration status of the outgoing Gratuitous ARP packets can be viewed using the `show arp send-gratuitous-arp` CLI command.

**Examples**

- `-> arp send-gratuitous-arp enable`
- `-> arp send-gratuitous-arp disable`

**Release History**

Release 8.7 R1; command introduced;

**Related Commands**

- `show arp send-gratuitous-arp` Displays if outgoing gratuitous ARP packets are enabled or disabled.
MIB Objects

alaIpArpSendGratuitous
clear arp-cache

Deletes all dynamic entries from the ARP table.

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command only clears dynamic entries. If permanent entries have been added to the table, they must be removed using the no form of the ip service command.
- Dynamic entries remain in the ARP table until they time out. The switch uses the MAC Address table timeout value as the ARP timeout value. Use the mac-learning aging-time command to set the timeout value.

Examples

-> clear arp-cache

Release History

Release 7.1.1; command introduced

Related Commands

- ip service
  Adds a permanent entry to the ARP table.
- show arp
  Displays the ARP table.

MIB Objects

- alaIpClearArpCache
**ip dos arp-poison restricted-address**

Adds or deletes an ARP Poison restricted address.

```plaintext
ip dos arp-poison restricted-address ip_address
no ip dos arp-poison restricted-address ip_address
```

---

**Syntax Definitions**

`ip_address` 32-bit IP address.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the `no` form of the command to remove an already configured ARP Poison restricted address.

---

**Examples**

```plaintext
-> ip dos arp-poison restricted-address 192.168.1.1
-> no ip dos arp-poison restricted-address 192.168.1.1
```

---

**Release History**

Release 7.1.1; command introduced

---

**Related Commands**

- `ip service` Adds a permanent entry to the ARP table.
- `show arp` Displays the ARP table.

---

**MIB Objects**

- `alaDoSArpPoisonTable`
  - `alaDoSArpPoisonIpAddr`
  - `alaDoSArpPoisonRowStatus`
arp filter

Configures an ARP filter that determines if ARP Request packets containing a specific IP address are processed by the switch or discarded.

**arp filter** *ip_address* [*mask ip_mask*] [*vlan_id*] [*sender | target*] [*allow | block*]

**no arp filter** *ip_address*

---

**Syntax Definitions**

- **ip_address**: The IP address to use for filtering ARP packet IP addresses.
- **ip_mask**: An IP mask that identifies which part of the ARP packet IP address is examined for filtering (for example, mask 255.0.0.0 filters on the first octet of the ARP packet IP address).
- **vlan_id**: A VLAN ID that specifies that only ARP packets for a specific VLAN are filtered.
- **sender**: The sender IP address in the ARP packet is used for ARP filtering.
- **target**: The target IP address in the ARP packet is used for ARP filtering.
- **allow**: ARP packets that meet filter criteria are processed.
- **block**: ARP packets that meet filter criteria are discarded.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id</td>
<td>0 (no VLAN)</td>
</tr>
<tr>
<td>ip_mask</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>sender</td>
<td>target</td>
</tr>
<tr>
<td>allow</td>
<td>block</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to delete an ARP filter.
- If there are no filters configured for the switch, all ARP Request packets received are processed.
- Up to 200 filters are allowed on each switch.
• If sender or target IP address in an ARP Request packet does not match any filter criteria, the packet is processed by the switch.

• ARP filtering is used in conjunction with the Local Proxy ARP application; however, ARP filtering is available for use on its own and/or with other applications.

**Examples**

-> arp filter 171.11.1.1
-> arp filter 172.0.0.0 mask 255.0.0.0
-> arp filter 198.0.0.0 mask 255.0.0.0 sender
-> arp filter 198.172.16.1 vlan 200 allow
-> no arp filter 171.11.1.1

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **clear arp filter** Clears all ARP filters from the filter database.
- **ip interface** Enables or disables the Local Proxy ARP feature on an IP interface. When enabled, all traffic within the VLAN is routed. ARP requests return the MAC address of the IP router interface.
- **show ip arp utilization** Displays the ARP filter configuration.

**MIB Objects**

alaIpArpFilterTable
  alaIpArpFilterIpAddr
  alaIpArpFilterIpMask
  alaIpArpFilterVlan
  alaIpArpFilterMode
  alaIpArpFilterType
clear arp filter

Clears the ARP filter database of all entries.

**clear arp-filter**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command clears all ARP filters configured on the switch. To remove an individual filter entry, use the `no` form of the `arp filter` command.

**Examples**

```
-> clear arp filter
```

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **arp filter**
  Configures an ARP filter to allow or block the processing of specified ARP Request packets.
- **show ip arp utilization**
  Displays the ARP filter configuration.

**MIB Objects**

- `alaIpClearArpFilter`
icmp type

Enables or disables a specific type of ICMP message, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

**Syntax**

```
icmp type type code code {enable | disable | min-pkt-gap gap}
```

**Syntax Definitions**

- **type**: The ICMP packet type. This is conjunction with the ICMP code that determines the type of ICMP message being specified.
- **code**: The ICMP code type. This is conjunction with the ICMP type that determines the type of ICMP message being specified.
- **enable**: Enables the specified ICMP message.
- **disable**: Disables the specified ICMP message.
- **gap**: The number of microseconds required between ICMP messages of this type.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>gap</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command allows the user to enable or disable all types of ICMP messages, and set the minimum packet gap between messages of the specified type.

- Enabling **Host unreachable** and **Network unreachable** messages are not recommended as it can cause the switch instability due to high-CPU conditions depending upon the volume of traffic required by these messages.

- While this command can be used to enable or disable all ICMP message, some of the more common ICMP messages have their own CLI commands, as described in the pages below. The following ICMP messages have specific commands to enable and disable:
ICMP Message | Command
---|---
Network unreachable (type 0, code 3) | icmp unreachable
Host unreachable (type 3, code 1) | icmp unreachable
Protocol unreachable (type 3, code 2) | icmp unreachable
Port unreachable (type 3, code 3) | icmp unreachable
Echo reply (type 0, code 0) | icmp echo
Echo request (type 8, code 0) | icmp echo
Timestamp request (type 13, code 0) | icmp timestamp
Timestamp reply (type 14, code 0) | icmp timestamp
Address Mask request (type 17, code 0) | icmp addr-mask
Address Mask reply (type 18, code 0) | icmp addr-mask

**Examples**

-> icmp type 4 code 0 enabled
-> icmp type 4 code 0 min-pkt-gap 40
-> icmp type 4 code 0 disable

**Release History**

Release 7.1.1; command introduced

**Related Commands**

* icmp messages* Enables or disables all ICMP messages.
* show arp send-gratuitous-arp* Allows the viewing of the ICMP control settings.

**MIB Objects**

alaIcmpCtrlTable
  alaIcmpCtrlType
alaIcmpCtrlTable
  alaIcmpCtrlCode
alaIcmpCtrlStatus
alaIcmpCtrlPktGap
### icmp unreachable

Enables or disables ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

```
icmp unreachable [net-unreachable | host-unreachable | protocol-unreachable | port-unreachable] {{enable | disable} | min-pkt-gap gap}
```

#### Syntax Definitions

- **net-unreachable**: Sets the unreachable network ICMP message.
- **host-unreachable**: Sets the unreachable host ICMP message.
- **protocol-unreachable**: Sets the unreachable protocol ICMP message.
- **port-unreachable**: Sets the unreachable port ICMP message.
- **enable**: Enables the specified ICMP message.
- **disable**: Disables the specified ICMP message.
- **gap**: The number of microseconds required between ICMP messages of this type.

#### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>gap</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- This command enables ICMP messages relating to unreachable destinations. Unreachable networks, hosts, protocols, and ports can all be specified.
- Enabling **host-unreachable** and **net-unreachable** messages are not recommended as it can cause the switch instability due to high-CPU conditions depending upon the volume of traffic required by these messages.
- The unreachable ICMP messages can also be enabled, disabled, and modified using the `icmp type` command. See the `icmp type` command information on the type and code for the unreachable ICMP messages.
Examples

-> icmp unreachable net-unreachable enable
-> icmp unreachable host-unreachable enable
-> icmp unreachable protocol-unreachable enable
-> icmp unreachable port-unreachable enable
-> icmp unreachable port-unreachable min-pkt-gap 50

Release History

Release 7.1.1; command introduced

Related Commands

show arp send-gratuitous-arp  Allows the viewing of the ICMP control settings.

MIB Objects

alaIcmpCtrlTable
  alaIcmpCtrlType
alaIcmpCtrlTable
  alaIcmpCtrlCode
alaIcmpCtrlStatus
alaIcmpCtrlPktGap
**icmp echo**

Enables or disables ICMP echo messages, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

\[ \text{icmp echo } [\text{request} | \text{reply}] \{\{\text{enable} | \text{disable}\} | \text{min-pkt-gap} \text{ } \text{gap}\} \]

---

### Syntax Definitions

- **request**: Specifies the echo request ICMP message.
- **reply**: Specifies the echo reply ICMP message.
- **enable**: Enables the specified ICMP message.
- **disable**: Disables the specified ICMP message.
- **gap**: The number of microseconds required between ICMP messages of this type.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>disable</td>
</tr>
<tr>
<td>gap</td>
<td>0</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command sets the ICMP echo messages. An echo request is sent to a destination, and must be responded to with an echo reply message that contains the original echo request.
- Using this command without specifying a request or reply enables, disables, or sets the minimum packet gap for both types.
- The echo ICMP messages can also be enabled, disabled, and modified using the `icmp type` command. See the `icmp type` command information on the type and code for the echo ICMP messages.

### Examples

- `> icmp echo reply enable`
- `> icmp echo enable`
- `> icmp echo request enable`
- `> icmp echo request min-pkt-gap 50`
Release History
Release 7.1.1; command introduced

Related Commands
show arp send-gratuitous-arp  Allows the viewing of the ICMP control settings.

MIB Objects
alaIcmpCtrlTable
   alaIcmpCtrlType
alaIcmpCtrlTable
   alaIcmpCtrlCode
   alaIcmpCtrlStatus
   alaIcmpCtrlPktGap
**icmp timestamp**

Enables or disables ICMP timestamp messages, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

```
icmp timestamp [request | reply] [{enable | disable} | min-pkt-gap gap]
```

### Syntax Definitions

- **request** Specifies timestamp request messages.
- **reply** Specifies timestamp reply messages.
- **enable** Enables the specified ICMP message.
- **disable** Disables the specified ICMP message.
- **gap** The number of microseconds required between ICMP messages of this type.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>enable</td>
</tr>
<tr>
<td>gap</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The data received (a timestamp) in the message is returned in the reply together with an additional timestamp. The timestamp is 32 bits of milliseconds since midnight UT. The Originate timestamp is the time the sender last touched the message before sending it, the Receive timestamp is the time the echoer first touched it on receipt, and the Transmit timestamp is the time the echoer last touched the message on sending it.

- Using this command without specifying a request or reply enables, disables, or sets the minimum packet gap for both types.

- The timestamp ICMP messages can also be enabled, disabled, and modified using the `icmp type` command. See the `icmp type` command information on the type and code for the timestamp ICMP messages.
Examples

-> icmp timestamp reply enable
-> icmp timestamp enable
-> icmp timestamp request enable
-> icmp timestamp request min-pkt-gap 50

Release History

Release 7.1.1; command introduced

Related Commands

show arp send-gratuitous-arp  Allows the viewing of the ICMP control settings.

MIB Objects

alaIcmpCtrlTable
  alaIcmpCtrlType
alaIcmpCtrlTable
  alaIcmpCtrlCode
  alaIcmpCtrlStatus
  alaIcmpCtrlPktGap
icmp addr-mask

Enables or disables ICMP address mask messages, and sets the minimum packet gap. The minimum packet gap is the number of microseconds that must pass between ICMP messages of the same type.

`icmp add-mask [request | reply] [{enable | disable} | min-pkt-gap gap]`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>request</td>
<td></td>
</tr>
<tr>
<td>reply</td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td></td>
</tr>
<tr>
<td>gap</td>
<td></td>
</tr>
</tbody>
</table>

request

Specifies request address mask messages.

reply

Specifies reply address mask messages.

enable

Enables the specified ICMP message.

disable

Disables the specified ICMP message.

gap

The number of microseconds required between ICMP messages of this type.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td></td>
</tr>
<tr>
<td>gap</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- A gateway receiving an address mask request must return it with the address mask field set to the 32-bit mask of the bits identifying the subnet and network, for the subnet on which the request was received.

- Using this command without specifying a request or reply enables, disable, or set the minimum packet gap for both types.

- The address mask ICMP messages can also be enabled, disabled, and modified using the `icmp type` command. See the `icmp type` command information on the type and code for the address mask ICMP messages.

---

**Examples**

- `-> icmp addr-mask reply enable`
- `-> icmp addr-mask enable`
-> icmp addr-mask request enable
-> icmp addr-mask request min-pkt-gap 50

**Release History**
Release 7.1.1; command introduced

**Related Commands**

*show arp send-gratuitous-arp*  Allows the viewing of the ICMP control settings.

**MIB Objects**
alaIcmpCtrlTable
  alaIcmpCtrlType
alaIcmpCtrlTable
  alaIcmpCtrlCode
  alaIcmpCtrlStatus
  alaIcmpCtrlPktGap
**icmp messages**

Enables or disables all Internet Control Message Protocol (ICMP) messages.

`icmp messages {enable | disable}`

---

**Syntax Definitions**

- **enable**  
  Enables ICMP messages.

- **disable**  
  Disables ICMP messages.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `-> icmp messages enable`
- `-> icmp messages disable`

**Release History**

Release 7.1.1; command introduced
**Related Commands**

- `icmp type` Enables or disables a specific type of ICMP message, and sets the minimum packet gap.
- `show arp send-gratuitous-arp` Allows the viewing of the ICMP control settings.

**MIB Objects**

- `alaIcmpCtrl`
- `alaIcmpAllMsgStatus`
**ip dos scan close-port-penalty**

Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.

**ip dos scan close-port-penalty penalty_value**

### Syntax Definitions

**penalty_value**

A penalty value added to the penalty scan value. This value can be any non-negative integer.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>penalty_value</td>
<td>10</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command creates a point value that is added to the total port scan penalty value when a TCP or UDP packet is received that is destined for a closed port.

### Examples

-> ip dos scan close-port-penalty 25

### Release History

Release 7.1.1; command introduced
Related Commands

- `ip dos scan threshold`  
  Sets the threshold for the port scan value, at which a DoS attack is recorded.

- `ip dos trap`  
  Sets whether the switch generates SNMP DoS traps when an attack is detected.

MIB Objects

- `alaDoSConfig`  
  - `alaDoSPortScanClosePortPenalty`
**ip dos scan tcp open-port-penalty**

Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP packet is received on an open port.

*ip dos scan tcp open-port-penalty penalty_value*

---

### Syntax Definitions

**penalty_value**

A penalty value added to the penalty scan value. This value can be any non-negative integer.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>penalty_value</td>
<td>0</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- This command creates a point value that is added to the total port scan penalty value when a TCP packet is received that is destined for an open port.
- The switch does not distinguish between a legal TCP packet and a port scan packet.

---

### Examples

`-> ip dos scan tcp open-port-penalty 10`

---

### Release History

Release 7.1.1; command introduced

---

### Related Commands

- **ip dos scan threshold**
  
  Sets the threshold for the port scan value, at which a DoS attack is recorded.

- **ip dos trap**
  
  Sets whether the switch generates SNMP DoS traps when an attack is detected.

---

### MIB Objects

- **alaDoSConfig**
alaDoSPortScanTcpOpenPortPenalty
ip dos scan udp open-port-penalty

Assigns a penalty value to be added to the Denial of Service penalty scan value when a UDP packet is received on an open port.

`ip dos scan udp open-port-penalty penalty_value`

### Syntax Definitions

| `penalty_value` | A penalty value added to the penalty scan value. This value can be any non-negative integer. |

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>penalty_value</code></td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command creates a point value that is added to the total port scan penalty value when a UDP packet is received that is destined for an open port.
- The switch does not distinguish between a legal UDP packet and a port scan packet.

### Examples

```
-> ip dos scan udp open-port-penalty 15
```

### Release History

Release 7.1.1; command introduced

### Related Commands

- `ip dos scan threshold` Sets the threshold for the port scan value, at which a DoS attack is recorded.
- `ip dos trap` Sets whether the switch generates SNMP DoS traps when an attack is detected.

### MIB Objects

`alaDoSConfig`
alaDoSPortScanUdpOpenPortPenalty
### ip dos scan threshold

Sets the threshold for the port scan value, at which a DoS attack is recorded.

**ip dos scan threshold** *threshold_value*

---

**Syntax Definitions**

*threshold_value* A numerical value representing the total acceptable penalty before a DoS attack is noted. This value can be any non-negative integer.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>threshold_value</em></td>
<td>1000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the total port scan penalty value exceeds this value, a port scan attack is recorded.
- The penalty value is incremented by recording TCP or UDP packets that are bound for open or closed ports. Such packets are given a penalty value, which are added. The commands for setting the packet penalty value are the *ip dos scan close-port-penalty*, *ip dos scan tcp open-port-penalty*, and *ip dos scan udp open-port-penalty* commands.

**Examples**

- `-> ip dos scan threshold 1200`

**Release History**

Release 7.1.1; command introduced
**Related Commands**

- `ip dos scan close-port-penalty`  
  Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP or UDP packet is received on a closed port.

- `ip dos scan tcp open-port-penalty`  
  Assigns a penalty value to be added to the Denial of Service penalty scan value when a TCP packet is received on an open port.

- `ip dos scan udp open-port-penalty`  
  Assigns a penalty value to be added to the Denial of Service penalty scan value when a UDP packet is received on an open port.

- `show ip dos config`  
  Displays the configuration parameters of the DoS scan for the switch.

**MIB Objects**

- `alaDoSConfig`  
  `alaDoSPortScanThreshold`
**ip dos trap**

Sets whether or not the switch generates SNMP DoS traps when an attack is detected.

```
ip dos trap {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the generation of DoS traps.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the generation of DoS traps.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command controls whether the switch generates an SNMP trap when a DoS attack is detected. It is assumed a DoS attack has occurred when the port scan penalty threshold is exceeded. This value is set using the `ip dos scan threshold` command.

### Examples

```
-> ip dos trap enable
-> ip dos trap disable
```

### Release History

Release 7.1.1; command introduced

### Related Commands

- `ip dos scan threshold` Sets the threshold for the port scan value, at which a DoS attack is recorded.
- `show ip dos config` Displays the configuration parameters of the DoS scan for the switch.
**MIB Objects**

alaDoSConfig

alaDoSTrapCnt1
ip dos scan decay

Sets the decay speed of the port scan penalty value for the switch when calculating DoS attacks.

**ip dos scan decay decay_value**

---

**Syntax Definitions**

- **decay_value**: The decay value amount for reducing the port scan penalty. This value can be any non-negative integer.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>decay_value</td>
<td>2</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The port scan penalty value is reduced every minute by dividing by the amount set in using this command. For example, if the decay value is set to 10, every minute the total port scan penalty value is divided by 10.

**Examples**

```
-> ip dos scan decay 10
```

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **ip dos scan threshold**: Sets the threshold for the port scan value, at which a DoS attack is recorded.
- **show ip dos config**: Displays the configuration parameters of the DoS scan for the switch.

**MIB Objects**

- **alaDoSConfig**
**ip dos type**

Enables or disables detection for the specified type of DoS attack.

```
ip dos type {port-scan | ping-of-death | land | loopback-src | invalid-ip | invalid-multicast | unicast-ip-mcast-mac | ping-overload | arp-flood | arp-poison | gratuitous-arp | ipoptions-filter} admin-state {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-scan</td>
<td>Detects port scans by monitoring TCP or UDP packets sent to open or closed ports.</td>
</tr>
<tr>
<td>ping-of-death</td>
<td>Detects the number of ICMP Ping-of-Death attacks (the switch receives ping packets that exceed the largest IP datagram size of 65535 bytes).</td>
</tr>
<tr>
<td>land</td>
<td>Detects the number of Land attacks (the switch receives spoofed packets with the SYN flag set on any open port that is listening).</td>
</tr>
<tr>
<td>loopback-src</td>
<td>Detects the number of loopback source attacks (the switch receives packets with 127.0.0.0/8 as the IP source address).</td>
</tr>
<tr>
<td>invalid-ip</td>
<td>Detects invalid IP packets (the switch receives packets with an invalid source or destination IP address).</td>
</tr>
<tr>
<td>invalid-multicast</td>
<td>Detects invalid Multicast packets (the switch receives packets with an invalid multicast address).</td>
</tr>
<tr>
<td>unicast-ip-mcast-mac</td>
<td>Detects a unicast IP and multicast MAC mismatch (the switch receives IP packets with multicast/broadcast source mac-address, non-matching destination IP and mac-address).</td>
</tr>
<tr>
<td>ping-overload</td>
<td>Detects a ping overload attack (the switch is flooded with a large number of ICMP packets).</td>
</tr>
<tr>
<td>arp-flood</td>
<td>Detects ARP flooding (the switch is flooded with a large number of ARP requests).</td>
</tr>
<tr>
<td>arp-poison</td>
<td>Detects ARP poisoning (the switch receives replies to an ARP request generated by the switch for a user-specified restricted address).</td>
</tr>
<tr>
<td>gratuitous-arp</td>
<td>Detects the Gratuitous ARP packets entering the switch. The incoming Gratuitous ARP packets can be allowed or blocked.</td>
</tr>
<tr>
<td>ipoptions-filter</td>
<td>Detects the packets with the IP option entering the switch. The incoming IP option packets can be allowed or dropped.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables DoS attack detection.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables DoS attack detection.</td>
</tr>
</tbody>
</table>

### Defaults

By default, detection is enabled for all the specified IP DoS attack types, except for ping overload and gratuitous-arp.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipoptions-filter</td>
<td>disabled</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When detection is enabled for ping overload, the attack is not detected until the number of ICMP packets received exceeds 100 packets-per-second.

- ARP flooding is rate limited to 500 packets-per-second on the switch. As a result, ARP flooding is not detected until the number of ARP requests exceeds 500 packets-per-second.

- When detection is enabled for unicast IP/multicast MAC mismatches (unicast-ip-mcast-mac), ping overload attacks (ping-overload), or ARP flooding attacks (arp-flood), packets are not dropped when the attack is detected.

Examples

- ip dos type ping-overload admin-state enable
- ip dos type land admin-state disable
- ip dos type gratuitous-arp admin-state disable
- ip dos type ipoptions-filter admin-state enable

Release History

- Release 7.1.1; command introduced
- Release 8.7 R1: gratuitous-arp parameter added.
- Release 8.7 R2: ipoptions-filter parameter added.

Related Commands

- show ip dos config
  Displays the DoS scan configuration for the switch.
- show ip dos statistics
  Displays statistics for the detected DoS attacks.

MIB Objects

- alaDoSTable
  alaDoSType
  alaDoSStatus
**ip tcp half-open-timeout**

Configures the timeout periods for dropping half-open TCP connections.

```
ip tcp half-open-timeout timeout_value
```

**Syntax Definitions**

- `timeout_value` The timeout value in seconds. Current supported values are 3, 7, 15, 31 and 63.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout_value</td>
<td>63 seconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> ip tcp half-open-timeout 7
```

**Release History**

Release 8.4.1; command introduced

**Related Commands**

- `show ip tcp half-open-timeout` Displays the timeout value configured for half-open TCP sessions.

**MIB Objects**

- `systemServices`  
  - `systemServicesTcpHalfOpenTimeout`
**ip tcp time-stamp-response**

Allows to enable or disable the TCP time stamp response.

```
ip tcp time-stamp-response admin-state {enable | disable}
```

**Syntax Definitions**

- **enable**: Enables the TCP time stamp response on the switch.
- **disable**: Disables the TCP time stamp response on the switch.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> ip tcp time-stamp-response admin-state disable
-> ip tcp time-stamp-response admin-state enable
```

**Release History**

Release 8.7R2; command introduced

**Related Commands**

- `show ip tcp time-stamp-response` Displays the TCP time stamp response status.

**MIB Objects**

- `systemServices`
  - `systemServicesTcpTimestampResponse`
**show ip tcp time-stamp-response**

Displays the TCP time stamp response status.

```
show ip tcp time-stamp-response
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

N/A

**Examples**

```
-> show ip tcp time-stamp-response
Tcp Time Stamp Response : Enable.
```

**Release History**

Release 8.7R2; command introduced

**Related Commands**

- `ip tcp time-stamp-response` Allows to enable or disable the TCP time stamp response.

**MIB Objects**

- `systemServicesTcptimestampresponse`
show ip traffic

Displays IP datagram traffic and errors.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The statistics show the cumulative totals since the last time the switch was powered on or since the last reset of the switch was executed.
- Packets received on a port that is a member of the UserPorts group are dropped if they contain a source IP network address that does not match the IP subnet for the port. This is done to block spoofed IP traffic. If the UserPorts group function is active and spoofed traffic was detected and blocked, the output display of this command includes statistics regarding the spoofed traffic.
- The presence of spoofing event statistics in the output display of this command indicates that an attack was prevented, not that the switch is currently under attack.
- If statistics for spoofed traffic are not displayed, then a spoofing attempt has not occurred since the last time this command was issued.

Examples

-> show ip traffic

Summary:
Datagrams received
  Total received = 621883,
  IP header error = 0,
  Destination IP error = 51752,
  Unknown protocol = 0,
  Local discards = 0,
  Delivered to users = 567330,
  Reassemble needed = 0,
Reassembled = 0,
Reassemble failed = 0

Datagrams sent
Forwarded = 2801,
Generated = 578108,
Local discards = 0,
No route discards = 9,
Fragmented = 2801,
Fragment failed = 0,
Fragments generated = 0

output definitions

Total
Total number of input datagrams received including the datagrams received in the error.

IP header error
Number of IP datagrams discarded due to errors in the IP header (for example, bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discarded in processing IP options).

Destination IP error
Number of IP datagrams discarded because the IP header destination field contained an invalid address. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported classes (for example, Class E).

Unknown protocol
Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Local discards
Number of IP datagrams received that were discarded, even though they had no errors to prevent transmission (for example, lack of buffer space). This does not include any datagrams discarded while awaiting reassembly. This value must be zero.

Delivered to users
Total number of datagrams received that were successfully delivered to IP user protocols (including ICMP).

Reassemble needed
Number of IP fragments received that needed to be reassembled.

Reassembled
Number of IP datagrams received that were successfully reassembled.

Reassemble failed
Number of IP failures detected by the IP reassembly algorithm for all reasons (for example, timed out, error). This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

Fragmented
Number of successfully fragmented IP datagrams.

Fragment failed
Number of packets received and discarded by IP that were not fragmented. This situation can happen if a large packet has the “Don’t Fragment” flag set.

Forwarded
Number of IP datagrams forwarded by the switch.

Generated
Total number of IP datagrams that local IP user protocols (including ICMP) generated in response to requests for transmission. This does not include any datagrams counted as “Forwarded.”

Local discards
Number of output IP datagrams that were discarded, even though they had no errors to prevent transmission (for example, lack of buffer space). This number includes datagrams counted as “Forwarded” if the packets are discarded for these reasons.
### Output Definitions (Continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No route discards</td>
<td>Number of IP datagrams received and discarded by IP because no route could be found to transmit them to their destination. This includes any packets counted as “Forwarded” if the packets are discarded for these reasons. It also includes any datagrams that a host cannot route because all of its default routers are down.</td>
</tr>
<tr>
<td>Fragments generated</td>
<td>The number of IP datagram fragments generated as a result of fragmentation.</td>
</tr>
<tr>
<td>Routing entry discards</td>
<td>Number of packets received and discarded by IP even though no problems were encountered to prevent their transmission to their destination (for example, discarded because of lack of buffer space).</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command introduced

### Related Commands

- **Show icmp statistics**
  - Displays ICMP statistics and errors.

### MIB Objects

- N/A
**show ip interface**

Displays the configuration and status of IP interfaces.

```
show ip interface [if_name | vlan vlan_id | dhcp-client]
```

**Syntax Definitions**

- **if_name**: The name associated with the IP interface.
- **vlan_id**: VLAN ID (displays a list of IP interfaces associated with a VLAN).
- **dhcp-client**: Displays the configuration and status of a DHCP Client interface.

**Defaults**

By default, all IP interfaces are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the optional **vlan** parameter to display a list of interfaces configured for the specified VLAN.
- Use the optional **if_name** parameter to display detailed information about an individual interface.
- Use the optional **dhcp-client** parameter to display detailed information about an interface that has been configured to obtain an IP address from a DHCP server.
- In a virtual chassis environment this command does not accurately reflect the status of the EMP IP interface on other chassis when entered on a Slave chassis.

**Examples**

```
-> show ip interface
Total 13 interfaces
  Flags (D=Directly-bound)
  Name         IP Address    Subnet Mask   Status  Forward Device   Flags
----------------------+-------------+-------------+--------+---------------------+------
EMP                    172.22.16.115 255.255.255.0     UP     NO EMP          +-----
UNP-RULE               40.1.1.1      255.255.255.0   DOWN    NO vlan 40     +-----
Loopback               127.0.0.1      255.0.0.0     UP     NO Loopback    +-----
L3VPN-2000             11.1.1.1      255.255.255.0     UP   YES service 1  +-----
L3VPN-1000             47.1.1.1      255.255.255.0     UP   YES service 2  +-----
if222                  30.1.5.1      255.0.0.0     UP     YES vlan 222   +-----
```
show ip interface

```
-> show ip interface vlan-23
Interface Name = vlan-23
   SNMP Interface Index           =   13600007,
   IP Address                     =   23.23.23.1,
   Subnet Mask                    =   255.0.0.0,
   Broadcast Address              =   23.255.255.255,
   Device                         =   vlan 23,
   Encapsulation                  =   eth2,
   Forwarding                     =   enabled,
   Administrative State           =   enabled,
   Operational State              =   up,
   Maximum Transfer Unit          =   1500,
   ARP Count                      =   1,
   Router MAC                     =   2c:fa:a2:13:e4:02,
   Local Proxy ARP                =   disabled,
   Primary (config/actual)        =   no/yes
```

-> show ip interface L3VPN
Interface Name = L3VPN
```
output definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface name.</td>
<td>This is the name configured for the interface (for example, Accounting). EMP-CMMA-CHAS1 refers to the Ethernet Management Port. Loopback refers to a built-in loopback interface that provides a local host address for the switch.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the interface. Configured through the ip interface command.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>IP subnet mask for the interface IP address. Configured through the ip interface command.</td>
</tr>
<tr>
<td>Status</td>
<td>Interface status:</td>
</tr>
<tr>
<td></td>
<td>• UP—Interface is ready to pass packets.</td>
</tr>
<tr>
<td></td>
<td>• DOWN—Interface is down.</td>
</tr>
<tr>
<td>Forward</td>
<td>Indicates whether the interface is actively forwarding packets (YES or NO).</td>
</tr>
<tr>
<td>Device</td>
<td>The type of device bound to the interface:</td>
</tr>
<tr>
<td></td>
<td>• unbound—No device is bound to the interface.</td>
</tr>
<tr>
<td></td>
<td>• vlan—The VLAN ID that is bound to the interface.</td>
</tr>
<tr>
<td></td>
<td>• EMP—The Ethernet Management Port is bound to the interface.</td>
</tr>
<tr>
<td></td>
<td>• Loopback—A loopback interface is configured for testing.</td>
</tr>
<tr>
<td></td>
<td>• GRE tunnel—GRE tunnel is configured for the interface.</td>
</tr>
<tr>
<td></td>
<td>• IPIP tunnel—IPIP tunnel is configured for the interface.</td>
</tr>
<tr>
<td></td>
<td>• service—The service ID that is bound to this interface.</td>
</tr>
<tr>
<td>Flags</td>
<td>Indicates if a switch port or link aggregate is directly bound to the interface (D=Directly-bound). This flag displays for IP routed-port interfaces.</td>
</tr>
</tbody>
</table>
```
SNMP Interface Index = 13600003,  
IP Address = 47.1.1.1,  
Subnet Mask = 255.255.255.0,  
Broadcast Address = 47.1.1.255,  
Device = Service 1,  
Forwarding = enabled,  
Administrative State = enabled,  
Operational State = up,  
Maximum Transfer Unit = 1500,  
Router MAC = e8:e7:32:1d:4c:88

-> show ip interface rp-vlan850
Interface Name = rp-vlan850  
SNMP Interface Index = 13600004,  
IP Address = 37.2.2.1,  
Subnet Mask = 255.0.0.0,  
Broadcast Address = 37.255.255.255,  
Device = vlan 850,  
Encapsulation = eth2,  
Forwarding = disabled,  
Administrative State = enabled,  
Operational State = down,  
Operational State Reason = device-down,  
Maximum Transfer Unit = 1500,  
ARP Count = 0,  
Router MAC = 00:e0:b1:e7:09:a3,  
Local Proxy ARP = disabled,  
Primary (config/actual) = no/no  
Directly bound port = 1/1/2, tagged

-> show ip interface dhcp-client
Interface Name = dhcp-client  
SNMP Interface Index = 13600010,  
IP Address = 0.0.0.0,  
Subnet Mask = 0.0.0.0,  
Broadcast Address = 0.0.0.0,  
Device = vlan 1,  
Encapsulation = eth2,  
Forwarding = disabled,  
Administrative State = enabled,  
Operational State = down,  
Operational State Reason = unbound,  
Maximum Transfer Unit = 1500,  
ARP Count = 0,  
Router MAC = 2c:fa:a2:7a:a7:db,  
Local Proxy ARP = disabled,  
Primary (config/actual) = yes/yes  
Vsi Accept Filter = ,  
DHCP-CLIENT Parameter Details  
Dhcp Prefer Server = FALSE,  
Client Status = Discovery,  
Server IP = N.A.,  
Router Address = N.A.,  
Lease Time Remaining = N.A.,  
Option-60 = OmniSwitch-OS6560-P48Z16,  
HostName = OS6560,
### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Interface Index</td>
<td>Interface index.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address associated with the interface. Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>IP subnet mask for the interface. Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Broadcast Address</td>
<td>Broadcast address for the interface.</td>
</tr>
<tr>
<td>Device</td>
<td>The type of device bound to the interface:</td>
</tr>
<tr>
<td></td>
<td>• <code>unbind</code>—No device is bound to the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>vlan</code>—The VLAN ID that is bound to the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>EMP</code>—The Ethernet Management Port is bound to the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>loopback</code>—A loopback interface is configured for testing.</td>
</tr>
<tr>
<td></td>
<td>• <code>GRE tunnel</code>—GRE tunnel is configured for the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>IPIP tunnel</code>—IPIP tunnel is configured for the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>service</code>—The service ID that is bound to this interface.</td>
</tr>
<tr>
<td></td>
<td>Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>Displays the IP router encapsulation (<code>eth2</code> or <code>snap</code>) that the interface uses when routing packets. Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Forwarding</td>
<td>Indicates whether IP forwarding is active for the interface (enabled or disabled). Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Administrative State</td>
<td>Administrative state of the IP interface (enabled or disabled), which is independent of the state of the underlying device. Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Indicates whether the interface is active (up or down).</td>
</tr>
<tr>
<td>Operation State Reason</td>
<td>Indicates why the operational state of the interface is down:</td>
</tr>
<tr>
<td></td>
<td>• <code>unbind</code>—No device is bound to the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>device-down</code>—Device bound to the interface is down.</td>
</tr>
<tr>
<td></td>
<td>• <code>admin-down</code>—The admin state of the interface is down.</td>
</tr>
<tr>
<td></td>
<td>• <code>no-such-device</code>—Device does not exist.</td>
</tr>
<tr>
<td></td>
<td>• <code>no-router-mac</code>—No MAC address available for the interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>tunnel-src-invalid</code>—The source IP address of the tunnel is invalid.</td>
</tr>
<tr>
<td></td>
<td>• <code>tunnel-dst-unreachable</code>—The destination IP address of the tunnel is not reachable.</td>
</tr>
<tr>
<td></td>
<td>• <code>invalid-config</code>—The IP interface is bound to an unsupported configuration.</td>
</tr>
<tr>
<td></td>
<td>The <code>tunnel-src-invalid</code> and <code>tunnel-dst-unreachable</code> Operational State reasons apply only when the type of device bound to the interface is a GRE tunnel or IPIP tunnel.</td>
</tr>
<tr>
<td></td>
<td>The <code>invalid-config</code> Operational State reason applies only when the IP interface is bound to an SPB Control BVLAN.</td>
</tr>
<tr>
<td></td>
<td><strong>Operational State Reason</strong> field is only included in the display output when the operational state of the interface is down.</td>
</tr>
<tr>
<td>Maximum Transfer Unit</td>
<td>The Maximum Transmission Unit size set for the interface. Configured through the <code>vlan mtu-ip</code> command.</td>
</tr>
<tr>
<td>Router MAC</td>
<td>Switch MAC address assigned to the interface. Each interface assigned to the same VLAN shares the same switch MAC address.</td>
</tr>
<tr>
<td>Local Proxy ARP</td>
<td>Indicates whether Local Proxy ARP is active for the interface (enabled or disabled). Configured through the <code>ip interface</code> command.</td>
</tr>
</tbody>
</table>
### output definitions (continued)

| **Primary (config/actual)** | Indicates if the interface is the configured and/or actual primary interface for the device (VLAN, EMP, Loopback). If the actual status is set to `yes` and the config status is set to `no`, the interface is the default interface for the VLAN. Configured through the `ip interface` command. |
| **Directly bound port** | Displays the physical port or link aggregate that is directly bound to the interface. Configured through the `ip interface rtr-port` command. This field displays only when the interface is configured as an IP routed port interface. |
| **ARP Count** | Displays the number of ARP entries in the NI. |
| **DHCP-Client Parameter Details** | (The following parameters are only applicable to the ‘dhcp-client’ interface. Configured through the `ip interface dhcp-client` command.) |
| **Dhcp Prefer Server** | Indicates if the DHCP server preference option is enabled or disabled. |
| **Client Status** | DHCP Client Status (**In-active, Active**) |
| **Server IP** | The IP address of the DHCP server. |
| **Router Address** | The IP address of the DHCP router. |
| **Lease Time Remaining** | The lease time remaining for the DHCP client IP address. |
| **Option-60** | The option-60 string that will be included in DHCP discover or request packets. |
| **HostName** | The system name of the OmniSwitch. |

```
-> show ip interface ipip-1
Interface Name = ipip-1
    SNMP Interface Index     = 13600001,
    IP Address               = 25.25.25.1,
    Subnet Mask              = 255.255.255.0,
    Device                   = IPIP Tunnel,
    Tunnel Source Address    = 23.23.23.1
    Tunnel Destination Address = 23.23.23.2,
    Forwarding               = enabled,
    Administrative State     = enabled,
    Operational State        = up,
    Maximum Transfer Unit    = 1480,

-> show ip interface gre-1
Interface Name = gre-1
    SNMP Interface Index     = 13600002,
    IP Address               = 24.24.24.1,
    Subnet Mask              = 255.255.255.0,
    Device                   = GRE Tunnel,
    Tunnel Source Address    = 23.23.23.1
    Tunnel Destination Address = 23.23.23.2,
    Forwarding               = enabled,
    Administrative State     = enabled,
    Operational State        = down,
    Operational State Reason = unbound,
    Maximum Transfer Unit    = 1476,
```
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Interface Index</td>
<td>Interface index.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address associated with the interface. Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>IP subnet mask for the interface. Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Device</td>
<td>The type of device bound to the interface:</td>
</tr>
<tr>
<td>unbound</td>
<td>No device is bound to the interface.</td>
</tr>
<tr>
<td>vlan</td>
<td>The VLAN ID that is bound to the interface.</td>
</tr>
<tr>
<td>EMP</td>
<td>The Ethernet Management Port is bound to the interface.</td>
</tr>
<tr>
<td>Loopback</td>
<td>A loopback interface is configured for testing.</td>
</tr>
<tr>
<td>GRE tunnel</td>
<td>GRE tunnel is configured for the interface.</td>
</tr>
<tr>
<td>IPIP tunnel</td>
<td>IPIP tunnel is configured for the interface.</td>
</tr>
<tr>
<td>service</td>
<td>The service ID that is bound to this interface.</td>
</tr>
<tr>
<td>Tunnel Source Address</td>
<td>The source IP address for the tunnel.</td>
</tr>
<tr>
<td>Tunnel Destination Address</td>
<td>The destination IP address for the tunnel.</td>
</tr>
<tr>
<td>Forwarding</td>
<td>Indicates whether IP forwarding is active for the interface (<code>enabled</code> or <code>disabled</code>). Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Administrative State</td>
<td>Administrative state of the IP interface (<code>enabled</code> or <code>disabled</code>), which is independent of the state of the underlying device. Configured through the <code>ip interface</code> command.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Indicates whether the interface is active (<code>up</code> or <code>down</code>).</td>
</tr>
<tr>
<td>Operational State Reason</td>
<td>Indicates why the operational state of the interface is down:</td>
</tr>
<tr>
<td>interface-up</td>
<td>The admin state of the interface is up.</td>
</tr>
<tr>
<td>unbound</td>
<td>No device is bound to the interface.</td>
</tr>
<tr>
<td>device-down</td>
<td>Device bound to the interface is down.</td>
</tr>
<tr>
<td>admin-down</td>
<td>The administrative state of the interface is down.</td>
</tr>
<tr>
<td>no-such-device</td>
<td>Device does not exist.</td>
</tr>
<tr>
<td>no-router-mac</td>
<td>No MAC address available for the interface.</td>
</tr>
<tr>
<td>tunnel-src-invalid</td>
<td>The source IP address of the tunnel is invalid.</td>
</tr>
<tr>
<td>tunnel-dst-unreachable</td>
<td>The destination IP address of the tunnel is not reachable.</td>
</tr>
<tr>
<td>Maximum Transfer Unit</td>
<td>The Maximum Transmission Unit size set for the interface. Configured through the <code>vlan mtu-ip</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

- Release 7.1.1; command introduced
- Release 7.3.4; output modified to display *Designated NI* and *ARP Count*.
- Release 8.5R1; *Dhcp prefer server* field added in output.
**Related Commands**

**ip interface**

Configures an IP interface to enable IP routing on a VLAN. Without an IP interface, traffic is bridged within the VLAN or across connections to the same VLAN on other switches.

**ip interface tunnel**

Configures the end points for the GRE and IPIP tunnels.

**show ip emp-interfaces**

Displays the configuration and status of the Ethernet Management Port (EMP) interface.

**show icmp statistics**

Displays ICMP statistics and errors.

**MIB Objects**

alaIpInterfaceTable

alaIpInterfaceName
alaIpInterfaceAddress
alaIpInterfaceMask
alaIpInterfaceAdminState
alaIpInterfaceDeviceType
alaIpInterfaceVlanID
alaIpInterfaceIpForward
alaIpInterfaceEncap
alaIpInterfaceLocalProxyArp
alaIpInterfacePrimCfg
alaIpInterfaceOperState
alaIpInterfaceOperReason
alaIpInterfaceRouterMac
alaIpInterfaceBcastAddr
alaIpInterfacePrimAct
alaIpInterfaceMtu
alaIpInterfaceTunnelSrc
alaIpInterfaceTunnelDst
alaIpInterfaceArpCount
alaIpInterfacePortIfindex
alaIpInterfaceTag
**show ip emp-interfaces**

Displays the configuration and status of the Ethernet Management Port (EMP) interface.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ip emp-routes` to display IP routes associated with the EMP interface.

**Examples**

```
-> show ip emp-interfaces
Total 1 interfaces
  Flags (D=Directly-bound)

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Status</th>
<th>Forward</th>
<th>Device</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMP-CMMA-CHAS1</td>
<td>3.3.3.25</td>
<td>255.0.0.0</td>
<td>DOWN</td>
<td>NO</td>
<td>EMP</td>
<td></td>
</tr>
</tbody>
</table>
```

**Name**

Interface name. `EMP-CMMA-CHAS1` refers to the Ethernet Management Port.

**IP Address**

IP address of the interface. Configured through the `ip interface` command.

**Subnet Mask**

IP subnet mask for the interface IP address. Configured through the `ip interface` command.

**Status**

Interface status:
- **UP**—Interface is ready to pass packets.
- **DOWN**—Interface is down.

**Forward**

Indicates whether the interface is actively forwarding packets (YES or NO).
**Device**
- **EMP**—The Ethernet Management Port is bound to the interface.

**Flags**
- N/A for EMP interfaces.

**Release History**
Release 7.3.3; command introduced.

**Related Commands**
- **show ip interface**
  Displays the status and configuration of IP interfaces.

**MIB Objects**
- N/A
show ip routes

Displays the IP Forwarding table.

[vrf vrf_name] show ip routes [summary]

Syntax Definitions

vrf_name The alphanumeric name (1–20 characters) assigned to the VRF instance.

summary Displays a summary of routing protocols that appear in the IP Forwarding table.

Defaults

By default, all routes are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The IP Forwarding table includes static routes as well as all routes learned through routing protocols (for example, RIP, OSPF).

- Use the optional summary keyword to display a list of routing protocols and the number of routes for each protocol that appear in the IP Forwarding table.

- The imported routes are also displayed under the protocol field as IMPORT in the show output.

Examples

-> show ip routes

+ = Equal cost multipath routes

Total 7 routes

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Gateway Addr</th>
<th>Age</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1/32</td>
<td>1.1.1.1</td>
<td>4d 5h</td>
<td>LOCAL</td>
</tr>
<tr>
<td>11.0.0.0/24</td>
<td>20.0.0.9</td>
<td>00:10:52</td>
<td>SPB-MGMT</td>
</tr>
<tr>
<td>20.0.0.0/8</td>
<td>20.0.0.1</td>
<td>4d 5h</td>
<td>LOCAL</td>
</tr>
<tr>
<td>24.0.0.0/8</td>
<td>0.0.0.0</td>
<td>4d 5h</td>
<td>STATIC</td>
</tr>
<tr>
<td>40.0.0.0/8</td>
<td>40.0.0.1</td>
<td>4d 5h</td>
<td>LOCAL</td>
</tr>
<tr>
<td>44.0.0.0/8</td>
<td>20.44.44.44</td>
<td>4d 5h</td>
<td>STATIC</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>127.0.0.1</td>
<td>4d 5h</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>
-> show ip routes summary

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Route Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>2</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
<tr>
<td>RIP</td>
<td>0</td>
</tr>
<tr>
<td>ISIS</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>0</td>
</tr>
<tr>
<td>BGP</td>
<td>0</td>
</tr>
<tr>
<td>Import</td>
<td>0</td>
</tr>
<tr>
<td>SPB-MGMT</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>0</td>
</tr>
<tr>
<td>TOTAL</td>
<td>3</td>
</tr>
</tbody>
</table>

**Output Definitions**

- **Dest Addr**: Destination IP address/mask length.
- **Gateway Addr**: IP address of the gateway from which this address was learned. Gateway address `0.0.0.0` indicates an IPv4 blackhole route.
- **Age**: Age of the entry. If the entry is less than a day old, it is displayed in hh/mm/ss format. If it is more than a day old, it is displayed in dd/hh format (for example, a route that is 2 days and 12 hours old is displayed as 2d12h).
- **Protocol**: Protocol by which this IP address was learned (for example, RIP). “Local” indicates a local interface.
- **Route Count**: The number of routes that appear in the IP Forwarding table for each protocol type listed.

**Release History**

- Release 7.1.1; command introduced
- Release 7.3.1; vrf parameter added.
- Release 8.7R2; “SPB-MGMT” protocol added to the output display.

**Related Commands**

- **ping**: Used to test whether an IP destination can be reached from the local switch.
- **traceroute**: Used to find the path taken by an IP packet from the local switch to a specified destination.
- **show ip router database**: Displays a list of all routes (static and dynamic) that exist in the IP router database.
**MIB Objects**

ipCidrRouteTable
  ipCidrRouteDest
  ipCidrRouteMask
  ipCidrRouteTos
  ipCidrRouteNextHop
  ipCidrRouteIfIndex
  ipCidrRouteType
  ipCidrRouteProto
  ipCidrRouteAge
  ipCidrRouteInfo
  ipCidrRouteNextHopAS
  ipCidrRouteMetric1
  ipCidrRouteMetric2
  ipCidrRouteMetric3
  ipCidrRouteMetric4
  ipCidrRouteMetric5
  ipCidrRouteStatus
show ip route-pref

Displays the IPv4 routing preferences of a router.

[vrf vrf_name] show ip route-pref

Syntax Definitions

vrf_name

The alphanumeric name (1–20 characters) assigned to the VRF instance.

 Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

By default, ISIS Level 1 routes are preferred over ISIS Level 2 routes and EBGP routes will carry a higher precedence than IBGP routes.

Examples

-> show ip route-pref

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Route Preference Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>1</td>
</tr>
<tr>
<td>Static</td>
<td>2</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>ISISL1</td>
<td>115</td>
</tr>
<tr>
<td>ISISL2</td>
<td>118</td>
</tr>
<tr>
<td>RIP</td>
<td>120</td>
</tr>
<tr>
<td>SPB-MGMT</td>
<td>150</td>
</tr>
<tr>
<td>EBGP</td>
<td>190</td>
</tr>
<tr>
<td>IBGP</td>
<td>200</td>
</tr>
<tr>
<td>Import</td>
<td>210</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced
Release 7.3.1; vrf parameter added.
Release 8.7R2; “SPB-MGMT” protocol added to the output display.
**Related Commands**

*ip route-pref*  
Configures the route preference of a router.

**MIB Objects**

alaIprmRtPrefTable

alaIprmRtPrefEntryType
alaIprmRtPrefEntryValue
show ip redist

Displays the IPv4 route map redistribution configuration.

[vrf vrf_name] show ip redist [rip | ospf | isis | bgp]

Syntax Definitions

vrf_name
The alphanumeric name (1–20 characters) assigned to the VRF instance.

rip
Displays route map redistribution configurations that use RIP as the destination (into) protocol.

ospf
Displays route map redistribution configurations that specify OSPF as the destination (into) protocol.

isis
Displays route map redistribution configurations that specify ISIS as the destination (into) protocol.

bgp
Displays the route map redistribution configurations that specify BGP as the destination (into) protocol at this time.

Defaults

By default, all route map redistribution configurations are shown.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify a destination protocol with this command to display only those configurations that redistribute routes into the specified protocol.

Examples

-> show ip redist

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Admin State</th>
<th>Route Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCAL4</td>
<td>OSPF</td>
<td>Enabled</td>
<td>auto-configure</td>
<td></td>
</tr>
<tr>
<td>STATIC4</td>
<td>SPB-MGMT</td>
<td>Enabled</td>
<td>route-map-spb-mgmt</td>
<td></td>
</tr>
<tr>
<td>RIP</td>
<td>OSPF</td>
<td>Enabled</td>
<td>ipv4rm</td>
<td></td>
</tr>
<tr>
<td>BGP</td>
<td>RIP</td>
<td>Enabled</td>
<td>ipv4fm</td>
<td></td>
</tr>
<tr>
<td>SPB-MGMT</td>
<td>OSPF</td>
<td>Enabled</td>
<td>none (all-routes)</td>
<td></td>
</tr>
<tr>
<td>IMPORT</td>
<td>RIP</td>
<td>Enabled</td>
<td>ipv4rm</td>
<td></td>
</tr>
</tbody>
</table>
-> show ip redist rip

<table>
<thead>
<tr>
<th>Source Protocol</th>
<th>Destination Protocol</th>
<th>Status</th>
<th>Route Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP</td>
<td>RIP</td>
<td>Enabled</td>
<td>ipv4rm</td>
</tr>
<tr>
<td>IMPORT</td>
<td>RIP</td>
<td>Enabled</td>
<td>ipv4rm</td>
</tr>
</tbody>
</table>

**output definitions**

- **Source Protocol**: The protocol from which the routes are learned.
- **Destination Protocol**: The protocol into which the source protocol routes are redistributed.
- **Status**: The administrative status (**Enabled** or **Disabled**) of the route map redistribution configuration.
- **Route Map**: The name of the route map that is applied with this redistribution configuration.

**Release History**

- Release 7.1.1; command introduced
- Release 7.3.1; vrf parameter added.
- Release 8.7R2; “SPB-MGMT” route redistribution included in the output display.

**Related Commands**

- `ip redist` Controls the conditions for redistributing different IPv4 routes between protocols.
- `show ip redist-routes` Displays all of the IPv6 routes that have been redistributed.

**MIB Objects**

- `alaRouteMapRedistProtoTable`
  - `alaRouteMapRedistSrcProtoId`
  - `alaRouteMapRedistDestProtoId`
  - `alaRouteMapRedistRouteMapIndex`
  - `alaRouteMapRedistStatus`
  - `alaRouteMapRedistAddressType`
  - `alaRouteMapRedistRowStatus`
show ip redist-routes

Displays all of the IPv4 routes that have been redistributed.

[vrf vrf_name] show ip redist-routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `show ip redist` command to display the IPv4 route redistribution configuration.

Examples

```
-> show ip redist-routes
Route Map    Route          Gateway    Source   Dest Metric RtType Tag    LocalPref Community
------------+--------------+----------+--------+----+------+------+------+---------+---------
static-rip-1 100.100.2.0/24 50.10.11.2 STATIC4 RIP       1 NONE        0         0
ospf-rip-1   20.20.2.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.3.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.4.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.5.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.6.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.7.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.8.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.9.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.10.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.11.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
ospf-rip-1   20.20.12.0/24 50.10.31.2 OSPF     RIP       1 TYPE1       0         0
```

output definitions

<table>
<thead>
<tr>
<th>Route Map</th>
<th>The name of the route map that is applied with this redistribution.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route</td>
<td>The redistributed route.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the gateway on which this route was learned.</td>
</tr>
<tr>
<td>Source</td>
<td>The source protocol.</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest</td>
<td>The destination protocol.</td>
</tr>
<tr>
<td>Metric</td>
<td>RIP metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.</td>
</tr>
<tr>
<td>RtType</td>
<td>The type of route:</td>
</tr>
<tr>
<td></td>
<td>- NONE—no route type (for example, a static route).</td>
</tr>
<tr>
<td></td>
<td>- INTERNAL—OSPF/BGP internal routes.</td>
</tr>
<tr>
<td></td>
<td>- EXTERNAL—OSPF/BGP external routes.</td>
</tr>
<tr>
<td></td>
<td>- TYPE1—OSPF external Type-1 routes.</td>
</tr>
<tr>
<td></td>
<td>- TYPE2—OSPF external Type-2 routes.</td>
</tr>
<tr>
<td></td>
<td>- LEVEL1—IS-IS Level-1 routes only.</td>
</tr>
<tr>
<td></td>
<td>- LEVEL2—IS-IS Level-2 routes only.</td>
</tr>
<tr>
<td></td>
<td>- SPB-MGMT—Shortest Path Bridging management routes.</td>
</tr>
<tr>
<td>Tag</td>
<td>The tag value of the route.</td>
</tr>
<tr>
<td>LocalPref</td>
<td>The local route preference of a route being redistributed into BGP.</td>
</tr>
<tr>
<td>Community</td>
<td>The community name of a route being redistributed into BGP.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.4.1R03; command introduced.

**Related Commands**

- **ip redist** Controls the conditions for redistributing different IPv4 routes between protocols.
- **show ip redist** Displays the route map redistribution configuration.

**MIB Objects**

<table>
<thead>
<tr>
<th>MIB</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
show ip access-list

Displays the details of the access list.

show ip access-list [access_list_name]

Syntax Definitions

access_list_name Name of the access list.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the access_list_name is not specified in this command, all the access lists are displayed.

Examples

-> show ip access-list

<table>
<thead>
<tr>
<th>Name</th>
<th>Address / Prefix Length</th>
<th>Effect</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>al_3</td>
<td>10.0.0.0/8</td>
<td>permit</td>
<td>all-subnets</td>
</tr>
<tr>
<td>al_3</td>
<td>11.0.0.0/8</td>
<td>permit</td>
<td>all-subnets</td>
</tr>
<tr>
<td>al_4</td>
<td>1.0.0.0/8</td>
<td>permit</td>
<td>no-subnets</td>
</tr>
<tr>
<td>al_4</td>
<td>10.0.0.0/8</td>
<td>permit</td>
<td>all-subnets</td>
</tr>
</tbody>
</table>

-> show ip access-list al_4

<table>
<thead>
<tr>
<th>Name</th>
<th>Address / Prefix Length</th>
<th>Effect</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>al_4</td>
<td>1.0.0.0/8</td>
<td>permit</td>
<td>no-subnets</td>
</tr>
<tr>
<td>al_4</td>
<td>10.0.0.0/8</td>
<td>permit</td>
<td>all-subnets</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>Name of the access list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address/Prefix Length</td>
<td>IP address that belongs to the access list.</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Effect</th>
<th>Indicates whether the IP address is permitted or denied.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redistribution Control</td>
<td>Indicates the conditions specified for redistributing the matched routes.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced

**Related Commands**

- `ip access-list` Creates an access list for adding multiple IPv4 addresses to route maps.
- `ip access-list address` Adds multiple IPv4 addresses to the access list.

**MIB objects**

`alaRouteMapAccessListIndex`
`alaRouteMapAccessListAddressType`
`alaRouteMapAccessListAddress`
`alaRouteMapAccessListPrefixLength`
`alaRouteMapAccessListAction`
`alaRouteMapAccessListRedistControl`
**show ip route-map**

Displays the IP route maps configured on the switch.

```
show ip route-map [route_map_name]
```

---

**Syntax Definitions**

- **route_map_name**
  - The name of the specific route map.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

If the **route_map_name** is not specified in this command, all the route maps are displayed.

---

**Examples**

```
-> show ip route-map
Route Maps: configured: 1 max: 200
Route Map: Route_map1 Sequence Number: 50 Action permit
  match ip address 10.0.0.0/8 redist-control all-subnets permit
  set metric 100 effect replace
```

---

**Release History**

Release 7.1.1; command introduced

---

**Related Commands**

**ip route-map action**

Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.
**MIB Objects**

- `alaRouteMapRedistProtoTable`
  - `alaRouteMapRedistRouteMapIndex`
- `alaRouteMapTable`
  - `alaRouteMapIndex`
  - `alaRouteMapSequence`
  - `alaRouteMapType`
  - `alaRouteMapValue`
  - `alaRouteMapRowStatus`
show ip router database

Displays a list of all routes (static and dynamic) that exist in the IP router database. This database serves as a central repository where routes are first processed and where duplicate routes are compared to determine the best route for the Forwarding Routing Database. If a route does not appear in the IP router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

[vrf vrf_name] show ip router database [protocol type | gateway ip_address | dest {ip_address/prefixlen | ip_address}]

Syntax Definitions

vrf_name The alphanumeric name (1–20 characters) assigned to the VRF instance.
type Routing protocol type (local, static, import, OSPF, RIP, BGP, ISIS, or SPB-MGMT).
ip_address Destination IP address.
ip_address/prefixlen The destination IP address along with the prefix length of the routes processed for redistribution.

Defaults

By default, all routes are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Command options are not mutually exclusive. You can use them on the same command line to narrow and/or customize the output display of this command. For example, use the protocol and dest options to display only those routes that are of a specific protocol type and have the specified destination network.

- The IP forwarding table is derived from IP router database processing performed by the switch and contains only unique routes that the switch currently uses. Use the show ip route command to view the forwarding table.

- If an expected route does not appear in the IP forwarding table, use the show ip router database command to see if the switch knows about the route and/or if a duplicate route with a higher precedence was selected instead.

- The switch compares the protocol of duplicate routes to determine which one to use. Regardless of whether a route has a higher priority metric value, protocol determines precedence. Local routes are...
given the highest level of precedence followed by static, OSFP, RIP, then BGP routes. As a result, a route that is known to the switch does not appear in the IP forwarding table if a duplicate route with a higher protocol precedence exists.

- A list of inactive static routes is also included in the `show ip router database` output display. A route becomes inactive if the interface for its gateway goes down. Inactive routes are unable to get to their destination and further investigation is warranted to determine why their gateway is unavailable.

- Static routes that appear as inactive are not included in the main IP router database listing. If an inactive route becomes active, however, it is removed from the inactive list and added to the active route list.

- The imported routes are also displayed under the protocol field as IMPORT in the show output.

**Examples**

```
-> show ip router database
Legend: + indicates routes in-use  
b indicates BFD-enabled static route  
i indicates interface static route  
r indicates recursive static route, with following address in brackets

Total IPRM IPv4 routes: 9

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Interface</th>
<th>Protocol</th>
<th>Metric</th>
<th>Tag</th>
<th>Misc-Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ 20.0.0.0/8</td>
<td>20.0.0.1</td>
<td>ip20</td>
<td>LOCAL</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>+b 22.0.0.0/8</td>
<td>20.0.0.22</td>
<td>ip20</td>
<td>STATIC</td>
<td>4</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>20.0.0.9</td>
<td>ip20</td>
<td>RIP</td>
<td>22</td>
<td>0</td>
<td>(backup)</td>
</tr>
<tr>
<td>+ 33.0.0.0/8</td>
<td>20.0.0.9</td>
<td>ip20</td>
<td>STATIC</td>
<td>33</td>
<td>0</td>
<td>[22.0.0.33]</td>
</tr>
<tr>
<td>+i 44.0.0.0/8</td>
<td>20.0.0.1</td>
<td>ip20</td>
<td>STATIC</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>+ 55.0.0.0/24</td>
<td>20.0.0.9</td>
<td>ip30</td>
<td>SPB-MGMT</td>
<td>11</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>+ 127.0.0.1/32</td>
<td>127.0.0.1</td>
<td>Loopback</td>
<td>LOCAL</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>+ 135.28.4.0/8</td>
<td>172.28.4.1</td>
<td>EMP</td>
<td>LOCAL</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>+ 172.0.0.0/24</td>
<td>0.0.0.0</td>
<td>Loopback</td>
<td>STATIC</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Inactive Static Routes

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
<th>Tag</th>
<th>Misc-Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.0/8</td>
<td>8.4.5.3</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

-> show ip router database dest 10.212.62.0/24 protocol ospf

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Protocol</th>
<th>Metric</th>
<th>Tag</th>
<th>Misc-Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.212.62.0/24</td>
<td>10.212.60.27</td>
<td>OSPF</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>10.212.62.0/24</td>
<td>10.212.61.27</td>
<td>OSPF</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

**output definitions**

- **Destination**: Destination IP address. Also includes the mask prefix length notation after the address to indicate the subnet mask value. For example, `/24` indicates the destination IP address has a 24-bit mask (255.255.255.0).

- **Gateway**: IP address of the gateway from which this route was learned. Gateway address ‘0.0.0.0’ indicates an IPv4 blackhole route.

- **Interface**: The interface associated with the gateway.
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong></td>
<td>Protocol by which this IP address was learned: LOCAL, STATIC,</td>
</tr>
<tr>
<td></td>
<td>IMPORT, OSPF, RIP, BGP, IS-IS, SPB-MGMT.</td>
</tr>
<tr>
<td><strong>Metric</strong></td>
<td>RIP metric or cost (hop count) for the route. Indicates a</td>
</tr>
<tr>
<td></td>
<td>priority for the route. The lower the metric value, the</td>
</tr>
<tr>
<td></td>
<td>higher the priority.</td>
</tr>
<tr>
<td><strong>Tag</strong></td>
<td>The tag associated with the route.</td>
</tr>
<tr>
<td><strong>Misc-Info</strong></td>
<td>Any additional information about the route.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced  
Release 7.3.1; `vrf` parameter added.  
Release 8.7R2; “SPB-MGMT” routes included in the output display.

**Related Commands**

- `show ip routes` Displays the IP Forwarding table.

**MIB Objects**

`alaIprmRouteTable`
- `alaIprmRouteDest`  
- `alaIprmRouteMask`  
- `alaIprmRouteTos`  
- `alaIprmRouteNextHop`  
- `alaIprmRouteProto`  
- `alaIprmRouteMetric`  
- `alaIprmRoutePriority`
show ip emp-routes

Displays the IP routes associated with the Ethernet Management Port (EMP).

show ip emp-routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command displays the routes that are connected to the Ethernet Management Port (EMP).
- The EMP cannot handle routing protocols such as RIP or OSPF.
- The default route for the switch cannot be set up on the EMP.
- There is no dedicated routing table for the EMP interface. All management interfaces use the same routing table with EMP and non-EMP routes.

Examples

`-> show ip emp-routes`

<table>
<thead>
<tr>
<th>Dest Address</th>
<th>Subnet Mask</th>
<th>Gateway Addr</th>
<th>Age</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>127.0.0.1</td>
<td>255.255.255.255</td>
<td>127.0.0.1</td>
<td>2d 4h</td>
<td>LOCAL</td>
</tr>
<tr>
<td>172.17.1.10</td>
<td>255.255.255.255</td>
<td>10.255.11.225</td>
<td>1d 5h</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>

output definitions

- **Dest Addr**: Destination IP address.
- **Subnet Mask**: Destination IP address IP subnet mask.
- **Gateway Addr**: IP address of the gateway from which this address was learned.
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Age</strong></td>
<td>Age of the entry. If the entry is less than a day old, it is displayed in <code>hh/mm/ss</code> format. If it is more than a day old, it is displayed in <code>dd/hh</code> format (for example, a route that is 2 days and 12 hours old is displayed as <code>2d12h</code>).</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Protocol by which this IP address was learned (for example, RIP). NETMGT indicates a static route. LOCAL indicates a local interface.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **ping** Tests whether an IP destination can be reached from the local switch.
- **traceroute** Finds the path taken by an IP packet from the local switch to a specified destination.

**MIB Objects**

- **N/A**
**show ip config**

Displays IP configuration parameters.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ip config
IP directed-broadcast  =  OFF,
IP default TTL          =  64
```

**output definitions**

<table>
<thead>
<tr>
<th>IP directed-broadcast</th>
<th>Indicates whether the IP directed-broadcast feature is on or off.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP default TTL</td>
<td>IP default TTL interval.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced
**Related Commands**

- **ip directed-broadcast** Enables or disables IP directed broadcasts routed through the switch.
- **ip default-ttl** Sets TTL value for IP packets.

**MIB Objects**

N/A
**show ip protocols**

Displays switch routing protocol information and whether the protocol is loaded or not loaded.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> show ip protocols

IP Protocols

RIP status = Not Loaded,
OSPF status = Loaded,
ISIS status = Not Loaded,
BGP status = Not Loaded,
PIM status = Loaded,
DVMRP status = Not Loaded,
RIPng status = Not Loaded,
OSPF3 status = Not Loaded,
LDP status = Not Loaded,
VRFP status = Loaded,

**Release History**

Release 7.1.1; command introduced
Related Commands

- `ip interface dhcp-client` - Configures the router primary IP address.
- `ip router router-id` - Configures the router ID for the router.

MIB Objects

- `alaIpRouteSumTable` - 
- `alaIpRouteProtocol` -
show ip router-id

Displays the primary IP address and router ID of the switch, if configured.

show ip router-id

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ip router-id
Router ID = 1.1.1.1,
Primary addr = 31.0.0.1

output definitions

<table>
<thead>
<tr>
<th></th>
<th>The set routing ID. The router ID is how the router is identified in IP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td></td>
</tr>
<tr>
<td>Primary addr</td>
<td></td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced
**Related Commands**

- `ip interface dhcp-client` Configures the router primary IP address.
- `ip router router-id` Configures the router ID for the router.

**MIB Objects**

- `alaIpRouteSumTable`
- `alaIpRouteProtocol`
show ip service

Displays the status of TCP/UDP service ports.

show ip service

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

The display output from this command also includes the service port number.

Examples

```plaintext
-> show ip service
Name                  Port Status
----------------------+-------+---------
ftp                   21    enabled
ssh                   22    disabled
telnet                23    disabled
udp-relay             67    disabled
http                  80    disabled
network-time          123   disabled
snmp                  161   disabled
avlan-telnet          259   disabled
avlan-http            260   disabled
avlan-secure-http     261   disabled
secure_http           443   enabled
proprietary           1024  disabled
proprietary           1025  disabled
```

output definitions

**Name**

Name of the TCP/UDP service.
**Release History**

Release 7.1.1; command introduced

**Related Commands**

*ip service* Enables (opens) or disables (closes) well-known TCP/UDP service ports.

**MIB Objects**

- *alaIpServiceTable*
  - *alaIpServiceType*
  - *alaIpServicePort*
  - *alaIpServiceStatus*
- *alaIpPortServiceTable*
  - *alaIpPortServicePort*
  - *alaIpPortServiceStatus*

<table>
<thead>
<tr>
<th>Port</th>
<th>The TCP/UDP well-known port number associated with the service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the well-known service port: <strong>enabled</strong> (port is closed) or <strong>disabled</strong> (port is open).</td>
</tr>
</tbody>
</table>
show ip service source-ip

Displays the source IP interfaces configured for the applications.

[vrf vrf_name] show ip service source-ip

Syntax Definitions

vrf_name Name of the VRF.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

- show ip service source-ip

Legend: "-" no explicit configuration.

Application            Interface-name
-------------------------+-------------------------------
dns                     -
ftp                     ipVlan100
ldap                    Loopback0
ntp                     Loopback0
radius                  Loopback0
sflow                   -
snmp                    Loopback0
ssh                     ipVlan100
swlog                   -
tacacs                  -
telnet                  -
tftp                    ipVlan100
ptp                     -
output definitions

<table>
<thead>
<tr>
<th>Application</th>
<th>Name of the TCP/UDP service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface-name</td>
<td>The source IP configured for the application.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command introduced

Related Commands

**ip service source-ip**

Configures a user-defined source IP address as the outgoing IP interface for the IP service.

MIB Objects

alaIpServiceSourceIPTable

- alaIPServiceSourceIpAppIndex
- alaIPServiceSourceIpName
- alaIPServiceSourceIpRowStatus
show ip dos arp-poison

Displays the number of attacks detected for configured ARP poison restricted-addresses.

show ip dos arp-poison

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

\[ \rightarrow \text{show ip dos arp-poison} \]

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.1</td>
<td>0</td>
</tr>
<tr>
<td>192.168.1.2</td>
<td>0</td>
</tr>
<tr>
<td>192.168.1.3</td>
<td>0</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>IP Address</th>
<th>The configured ARP Poison restricted-addresses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attacks detected</td>
<td>The number of ARP Poison attacks detected for each address.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced
Related Commands

**ip dos arp-poison restricted-address**  Adds or deletes an ARP Poison restricted address.

MIB Objects

alaDoSArpPoisonTable
  alaDoSArpPoisonIpAddr
  alaDoSArpPoisonDetected
**show arp**

Displays the ARP table. The ARP table contains a listing of IP addresses and their corresponding translations to physical MAC addresses.

```
show arp [ip_address | mac_address]
```

**Syntax Definitions**

- `ip_address` - IP address of the entry you want to view.
- `mac_address` - MAC address of the entry you want to view.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the basic command (`show arp`) to view all of the entries in the table. Enter a specific IP address or MAC address to view a specific entry.

**Examples**

```
-> show arp

Total 11 arp entries
Flags (P=Proxy, A=Authentication, V=VRRP, B=BFD, H=HAVLAN, I=INTF, M=Managed)

<table>
<thead>
<tr>
<th>IP Addr</th>
<th>Hardware Addr</th>
<th>Type</th>
<th>Flags</th>
<th>Port</th>
<th>Interface</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.11.59</td>
<td>00:50:04:b2:c9:ee</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>10.255.11.48</td>
<td>00:50:04:b2:ca:11</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>10.255.11.201</td>
<td>00:10:83:03:e7:e4</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>10.255.11.14</td>
<td>00:10:5a:04:19:a7</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>10.255.11.64</td>
<td>00:b0:d0:62:fa:f1</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>10.255.11.25</td>
<td>00:b0:d0:42:80:24</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>10.255.11.26</td>
<td>00:b0:d0:42:82:59</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>20.0.0.22</td>
<td>e4:c2:33:00:21:12</td>
<td>STATIC</td>
<td>I</td>
<td>2/1/20</td>
<td>ip20</td>
<td>server1</td>
</tr>
<tr>
<td>10.255.11.254</td>
<td>00:20:da:db:00:47</td>
<td>DYNAMIC</td>
<td></td>
<td>1/1/20</td>
<td>vlan 1</td>
<td></td>
</tr>
<tr>
<td>40.1.1.1</td>
<td>e8:e7:32:1e:4c:88</td>
<td>STATIC</td>
<td>M</td>
<td>1/1/2</td>
<td>v4000</td>
<td></td>
</tr>
<tr>
<td>40.1.1.3</td>
<td>e2:e7:32:1e:4b:f8</td>
<td>STATIC</td>
<td>M</td>
<td>1/1/2</td>
<td>v4000</td>
<td></td>
</tr>
</tbody>
</table>
```
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Device IP address.</td>
</tr>
<tr>
<td>Hardware Addr</td>
<td>MAC address of the device that corresponds to the IP address.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates whether the ARP cache entries are dynamic or static.</td>
</tr>
<tr>
<td>Flags</td>
<td>Indicates the type of entry:</td>
</tr>
<tr>
<td></td>
<td>• P = Proxy</td>
</tr>
<tr>
<td></td>
<td>• A = Authentication (AVLAN)</td>
</tr>
<tr>
<td></td>
<td>• V = VRRP</td>
</tr>
<tr>
<td></td>
<td>• B = BFD</td>
</tr>
<tr>
<td></td>
<td>• H = HAVLAN</td>
</tr>
<tr>
<td></td>
<td>• I = INTF</td>
</tr>
<tr>
<td></td>
<td>• M = Managed</td>
</tr>
<tr>
<td>Port</td>
<td>The port on the switch attached to the device identified by the IP address.</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface to which the entry belongs (for example, VLAN, EMP).</td>
</tr>
<tr>
<td>Name</td>
<td>The name assigned to a static ARP entry.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **arp** Adds a permanent entry to the ARP table.
- **clear arp-cache** Deletes all dynamic entries from the ARP table.

**MIB Objects**

- `ipNetToMediaTable`
  - `ipNetToMediaIfIndex`
  - `ipNetToMediaNetAddress`
  - `ipNetToMediaPhyAddress`
  - `ipNetToMediaType`
- `ipNetToMediaAugTable`
  - `ipNetToMediaSlot`
  - `ipNetToMediaPort`
- `alaIpNetToMediaTable`
  - `alaIpNetToMediaPhyAddress`
  - `alaIpNetToMediaProxy`
  - `alaIpNetToMediaVRRP`
  - `alaIpNetToMediaAuth`
**show ip arp utilization**

Displays the designated NIs for the interfaces and the NI utilization.

**show ip arp utilization [slot chassis/slot | interfaces]**

---

**Syntax Definitions**

- **chassis/slot**: The chassis ID and slot number of the interface. The output is displayed specific to the slot.
- **interfaces**: Displays the ARP utilization of the designated-NI on all the configured interfaces.

---

**Defaults**

N/A

---

**Platforms Supported**

Not supported in this release.

---

**Usage Guidelines**

Use the basic command (**show ip arp utilization**) to view all of the entries in the table. Enter a specific chassis and slot number to view a specific entry.

---

**Examples**

```
-> show ip arp utilization
Distributed ARPs: Enabled

<table>
<thead>
<tr>
<th>NI</th>
<th>Max</th>
<th>ARP</th>
<th>HW</th>
<th>Count</th>
<th>Usage</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>16384</td>
<td>8</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
<tr>
<td>2/1</td>
<td>16384</td>
<td>12</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0%</td>
</tr>
</tbody>
</table>

-> show ip arp utilization interfaces
Distributed ARPs: Enabled

<table>
<thead>
<tr>
<th>NI</th>
<th>Max</th>
<th>ARP</th>
<th>HW</th>
<th>ARPS</th>
<th>%</th>
<th>VRF</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>16384</td>
<td>1</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>16384</td>
<td>5</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>16384</td>
<td>5</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>1/1</td>
<td>16384</td>
<td>5</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>16384</td>
<td>1</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>16384</td>
<td>5</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>16384</td>
<td>5</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>2/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>
```
show ip arp utilization slot 2/1/1

Distributed ARPs: Enabled

<table>
<thead>
<tr>
<th>NI</th>
<th>Max</th>
<th>ARP Count</th>
<th>HW Usage</th>
<th>%</th>
<th>VRF</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1/1</td>
<td>16384</td>
<td>1</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>2/1/1</td>
<td>16384</td>
<td>5</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>16</td>
</tr>
<tr>
<td>2/1/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>2/1/1</td>
<td>16384</td>
<td>5</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>18</td>
</tr>
<tr>
<td>2/1/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>19</td>
</tr>
<tr>
<td>2/1/1</td>
<td>16384</td>
<td>5</td>
<td>4</td>
<td>0%</td>
<td>0</td>
<td>20</td>
</tr>
</tbody>
</table>

**Output definitions**

- **NI**: The chassis ID and slot number of the designated-NI.
- **Max**: The maximum number of ARP entries supported on the NI.
- **ARP count**: ARP count in the NI for the NI or interface.
- **HW Usage**: The amount of table space used up in the ASIC.
- **HW ARPS**: The number of ARPs in the ASIC.
- **%**: The percentage of ARP utilization on that designated-NI.
- **VRF**: The name of the VRF associated to the interface.
- **Interface**: The interface to which the entry belongs.

**Release History**

Release 7.3.4; command introduced

**Related Commands**

- **ip distributed-arp admin-state**: Enables or disables the distributed ARP feature.

**MIB Objects**

- **alaDistArpNiTable**
  - **alaDistArpItfTable**
**show arp filter**

Displays a list of ARP filters configured for the switch.

```
show arp filter [ip_address]
```

### Syntax Definitions

- `ip_address` IP address of the filter entry you want to view.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If an IP address is not specified with this command, a list of all ARP filters is displayed.
- Enter a specific IP address to view the configuration for an individual filter.

### Examples

```
-> show arp filter
IP Addr   IP Mask   Vlan  Type    Mode
----------------+---------+-----+--------+-------
171.11.1.1     255.255.255.255  0    target block
172.0.0.0      255.0.0.0       0    target block
198.0.0.0      255.0.0.0       0    sender block
198.172.16.1   255.255.255.255 200  target allow

-> show arp filter 198.172.16.1
IP Addr   IP Mask   Vlan  Type    Mode
----------------+---------+-----+--------+-------
198.0.0.0      255.0.0.0       0    sender block
198.172.16.1   255.255.255.255 200  target allow
```

### Output Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Addr</td>
<td>The ARP packet IP address to which the filter is applied.</td>
</tr>
<tr>
<td>IP Mask</td>
<td>The IP mask that specifies which part of the IP address to which the filter is applied.</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan</td>
<td>A VLAN ID. The filter is applied only to ARP packets received on ports associated with this VLAN.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates which IP address in the ARP packet (sender or target) is used to identify if a filter exists for that address.</td>
</tr>
<tr>
<td>Mode</td>
<td>Indicates whether to block or allow a switch response to an ARP packet that matches the filter.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **arp filter**
  Adds a permanent entry to the ARP table.

- **clear arp filter**
  Deletes all dynamic entries from the ARP table.

**MIB Objects**

- alaIpArpFilterTable
  - alaIpArpFilterIpAddr
  - alaIpArpFilterIpMask
  - alaIpArpFilterVlan
  - alaIpArpFilterMode
  - alaIpArpFilterType
**show arp send-gratuitous-arp**

Displays whether outgoing gratuitous ARP packets are blocked or periodically sent by the switch.

**show arp send-gratuitous-arp**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```bash
-> show arp send-gratuitous-arp
Send Gratuitous ARP is disabled
```

**output definitions**

<table>
<thead>
<tr>
<th>Send Gratuitous ARP is disabled</th>
<th>The outgoing Gratuitous ARP packets are blocked.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send Gratuitous ARP is enabled</td>
<td>The switch can periodically send the Gratuitous ARP packets.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.7 R1; command introduced
Related Commands

arp send-gratuitous-arp

Enables or disables the outgoing Gratuitous ARP packets.

MIB Objects

alaIpArpSendGratuitous
**show icmp control**

Allows the viewing of the ICMP control settings.

show icmp control

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6450</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>X48C4E/V48C8</th>
<th>6900C32E/T24C2</th>
<th>9900X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to view the status of the various ICMP messages. It is also useful to determine the type and code of the less common ICMP messages.

**Examples**

```
-> show icmp control
Name                        Type Code Status  min-pkt-gap(us)
-------------------------------------+--------+---------+------------------
echo reply                   0   0     enabled     0
network unreachable           3   0     enabled     0
host unreachable              3   1     enabled     0
protocol unreachable          3   2     enabled     0
port unreachable              3   3     enabled     0
frag needed but DF bit set    3   4     enabled     0
source route failed           3   5     enabled     0
destination network unknown   3   6     enabled     0
destination host unknown      3   7     enabled     0
source host isolated          3   8     enabled     0
dest network admin prohibited 3   9     enabled     0
host admin prohibited by filter 3 10     enabled     0
network unreachable for TOS   3 11     enabled     0
host unreachable for TOS      3 12     enabled     0
source quench                 4   0     enabled     0
redirect for network          5   0     enabled     0
redirect for host             5   1     enabled     0
redirect for TOS and network  5   2     enabled     0
redirect for TOS and host     5   3     enabled     0
```
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Code</th>
<th>Status</th>
<th>min-pkt-gap</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo request</td>
<td>8</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>router advertisement</td>
<td>9</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>router solicitation</td>
<td>10</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>time exceeded during transmit</td>
<td>11</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>time exceeded during reassembly</td>
<td>11</td>
<td>1</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>ip header bad</td>
<td>12</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>required option missing</td>
<td>12</td>
<td>1</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>timestamp request</td>
<td>13</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>timestamp reply</td>
<td>14</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>information request(obsolete)</td>
<td>15</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>information reply(obsolete)</td>
<td>16</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>address mask request</td>
<td>17</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
<tr>
<td>address mask reply</td>
<td>18</td>
<td>0</td>
<td>enabled</td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

**Name**

The name of the ICMP message.

**Type**

The ICMP message type. This along with the ICMP code specifies the ICMP message.

**Code**

The ICMP message code. This along with the ICMP type specifies the ICMP message.

**Status**

Whether this message is **Enabled** or **Disabled**.

**min-pkt-gap**

The minimum packet gap, in microseconds, for this ICMP message.

The minimum packet gap is the amount of time that must pass between ICMP messages of like types.

---

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **icmp type**
  
  Enables or disables a specific type of ICMP message, and sets the minimum packet gap.

- **icmp unreachable**
  
  Enables or disables ICMP messages pertaining to unreachable destinations, and sets the minimum packet gap.

- **icmp echo**
  
  Enables or disables ICMP echo messages, and sets the minimum packet gap.

- **icmp timestamp**
  
  Enables or disables ICMP timestamp messages, and sets the minimum packet gap.

- **icmp addr-mask**
  
  Enables or disables ICMP address mask messages, and sets the minimum packet gap.

- **icmp messages**
  
  Enables or disables all ICMP messages.

**MIB Objects**

N/A
show icmp statistics

Displays Internet Control Message Protocol (ICMP) statistics and errors. ICMP is a network layer protocol within the IP protocol suite that provides message packets to report errors and other IP packet processing information back to the source. ICMP generates several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

show icmp [statistics]

Syntax Definitions

statistics Optional syntax.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the ICMP Table to monitor and troubleshoot the switch.

Examples

-> show icmp
Messages Received Sent
-----------------------------------------+-------------+-------------
Total                                  2105        2105
Error                                  0           0
Destination unreachable                0           0
Time exceeded                          0           0
Parameter problem                      0           0
Source quench                          0           0
Redirect                                0           0
Echo request                           2105        0
Echo reply                             0           2105
Time stamp request                     0           0
Time stamp reply                       0           0
Address mask request                   0           0
Address mask reply                     0           0
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Total number of ICMP messages the switch received or attempted to send. This counter also includes all the messages that were counted as errors.</td>
</tr>
<tr>
<td>Error</td>
<td>Number of ICMP messages the switch sent/received but was unable to process because of ICMP-specific errors (for example, bad ICMP checksums, bad length).</td>
</tr>
<tr>
<td>Destination unreachable</td>
<td>Number of “destination unreachable” messages that were sent/received by the switch.</td>
</tr>
<tr>
<td>Time exceeded</td>
<td>Number of “time exceeded” messages that were sent/received by the switch. These messages occur when a packet is dropped because the TTL counter reaches zero. When a large number of these messages occur, it is a symptom that packets are looping, that congestion is severe, or that the TTL counter value is set too low. These messages also occur when all the fragments trying to be reassembled do not arrive before the reassembly timer expires.</td>
</tr>
<tr>
<td>Parameter problem</td>
<td>Number of messages sent/received which indicate that an illegal value has been detected in a header field. These messages can indicate a problem in the sending IP software of the host or gateway.</td>
</tr>
<tr>
<td>Source quench</td>
<td>Number of messages sent/received that tell a host that it is sending too many packets. A host must attempt to reduce its transmissions upon receiving these messages.</td>
</tr>
<tr>
<td>Redirect</td>
<td>Number of ICMP redirect messages sent/received by the switch.</td>
</tr>
<tr>
<td>Echo request</td>
<td>Number of ICMP echo messages sent/received by the switch to see if a destination is active and unreachable.</td>
</tr>
<tr>
<td>Echo reply</td>
<td>Number of echo reply messages received by the switch.</td>
</tr>
<tr>
<td>Time stamp request</td>
<td>Number of time stamp request messages sent/received by the switch.</td>
</tr>
<tr>
<td>Time stamp reply</td>
<td>Number of time stamp reply messages sent/received by the switch.</td>
</tr>
<tr>
<td>Address mask request</td>
<td>Number of address mask request messages that were sent/received by the switch in an attempt to determine the subnet mask for the network.</td>
</tr>
<tr>
<td>Address mask reply</td>
<td>Number of address mask reply messages that were sent/received by the switch.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced

Related Commands

- **show udp statistics**: Displays UDP errors and statistics.

MIB Objects

N/A
**show tcp statistics**

Displays TCP statistics.

`show tcp statistics`

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show tcp statistics
Total segments received = 235080,
Error segments received = 0,
Total segments sent = 363218,
Segments retransmitted = 38,
Reset segments sent = 97,
Connections initiated = 57185,
Connections accepted = 412,
Connections established = 1,
Attempt fails = 24393,
Established resets = 221
```

**output definitions**

- **Total segments received**: Total number of segments received, including the segments received in the error. This count includes segments received on currently established connections.
- **Error segments received**: Total number of segments received in error (for example, bad TCP checksums).
- **Total segments sent**: Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
- **Segments retransmitted**: Number of TCP segments transmitted containing one or more previously transmitted octets.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset segments sent</td>
<td>Number of TCP segments containing the reset flag.</td>
</tr>
<tr>
<td>Connections initiated</td>
<td>Number of connections attempted.</td>
</tr>
<tr>
<td>Connections accepted</td>
<td>Number of connections allowed.</td>
</tr>
<tr>
<td>Connections established</td>
<td>Number of successful connections.</td>
</tr>
<tr>
<td>Attempt fails</td>
<td>Number of times attempted TCP connections have failed.</td>
</tr>
<tr>
<td>Established resets</td>
<td>Number of times TCP connections have been reset from the &quot;Established&quot; or &quot;Close Wait&quot; state to the “Closed” state.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced

**Related Commands**

- **show icmp statistics** Displays ICMP statistics and errors.
- **show tcp ports** Displays the TCP connection table.

**MIB Objects**

N/A
### show tcp ports

Displays the TCP connection table.

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this table to check the current available TCP connections.

### Examples

```
-> show tcp ports
Local Address   Local Port   Remote Address    Remote Port    State
--------------------------------------------------------------
0.0.0.0          21            0.0.0.0               0              LISTEN
0.0.0.0          23            0.0.0.0               0              LISTEN
0.0.0.0          80            0.0.0.0               0              LISTEN
0.0.0.0          260           0.0.0.0               0              LISTEN
0.0.0.0          261           0.0.0.0               0              LISTEN
0.0.0.0          443           0.0.0.0               0              LISTEN
0.0.0.0          6778          0.0.0.0               0              LISTEN
10.255.11.223   23            128.251.16.224        1867           ESTABLISHED
10.255.11.223   2509          10.255.11.33           389            TIME-WAIT
10.255.11.223   2510          10.255.11.25           389            TIME-WAIT
10.255.11.223   2513          10.255.11.33           389            TIME-WAIT
10.255.11.223   2514          10.255.11.25           389            TIME-WAIT
10.255.11.223   2517          10.255.11.33           389            TIME-WAIT
10.255.11.223   2518          10.255.11.25           389            TIME-WAIT
10.255.11.223   2521          10.255.11.33           389            TIME-WAIT
10.255.11.223   2522          10.255.11.25           389            TIME-WAIT
10.255.11.223   2525          10.255.11.33           389            TIME-WAIT
10.255.11.223   2526          10.255.11.25           389            TIME-WAIT
10.255.11.223   2529          10.255.11.33           389            TIME-WAIT
10.255.11.223   2530          10.255.11.25           389            TIME-WAIT
```
Output definitions

<table>
<thead>
<tr>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Address</td>
<td>Local IP address for this TCP connection. If a connection is in the</td>
</tr>
<tr>
<td></td>
<td>LISTEN state it accepts connections for any IP interface associated</td>
</tr>
<tr>
<td></td>
<td>with the node. The IP address 0.0.0.0 is used.</td>
</tr>
<tr>
<td>Local Port</td>
<td>Local port number for this TCP connection. The range is 0–65535.</td>
</tr>
<tr>
<td>Remote Address</td>
<td>Remote IP address for this TCP connection.</td>
</tr>
<tr>
<td>Remote Port</td>
<td>Remote port number for this TCP connection. The range is 0–65535.</td>
</tr>
<tr>
<td>State</td>
<td>State of the TCP connection, as defined in RFC 793. A connection</td>
</tr>
<tr>
<td></td>
<td>progresses through a series of states during its lifetime:</td>
</tr>
<tr>
<td></td>
<td>• Listen—Waiting for a connection request from any remote TCP</td>
</tr>
<tr>
<td></td>
<td>and port.</td>
</tr>
<tr>
<td></td>
<td>• Syn Sent—Waiting for a matching connection request after having</td>
</tr>
<tr>
<td></td>
<td>sent a connection request.</td>
</tr>
<tr>
<td></td>
<td>• Syn Received—Waiting for a confirming connection request</td>
</tr>
<tr>
<td></td>
<td>acknowledgment after having both received and sent a connection</td>
</tr>
<tr>
<td></td>
<td>request.</td>
</tr>
<tr>
<td></td>
<td>• Established—Open connection. Data received can be delivered to</td>
</tr>
<tr>
<td></td>
<td>the user. This is the normal state for the data transfer phase of</td>
</tr>
<tr>
<td></td>
<td>the connection.</td>
</tr>
<tr>
<td></td>
<td>• Fin Wait 1—Waiting for a connection termination request from the</td>
</tr>
<tr>
<td></td>
<td>remote TCP, or an acknowledgment of the connection termination</td>
</tr>
<tr>
<td></td>
<td>request previously sent.</td>
</tr>
<tr>
<td></td>
<td>• Fin Wait 2—Waiting for a connection termination request from the</td>
</tr>
<tr>
<td></td>
<td>remote TCP.</td>
</tr>
<tr>
<td></td>
<td>• Close Wait—Waiting for a connection termination request from the</td>
</tr>
<tr>
<td></td>
<td>local user.</td>
</tr>
<tr>
<td></td>
<td>• Closing—Waiting for a connection termination request acknowledgment</td>
</tr>
<tr>
<td></td>
<td>from the remote TCP.</td>
</tr>
<tr>
<td></td>
<td>• Last Ack—Waiting for an acknowledgment of the connection termination</td>
</tr>
<tr>
<td></td>
<td>request previously sent to the remote TCP (which includes an</td>
</tr>
<tr>
<td></td>
<td>acknowledgment of its connection termination request).</td>
</tr>
<tr>
<td></td>
<td>• Time Wait—Waiting for enough time to pass to be sure the remote</td>
</tr>
<tr>
<td></td>
<td>TCP received the acknowledgment of its connection termination</td>
</tr>
<tr>
<td></td>
<td>request.</td>
</tr>
<tr>
<td></td>
<td>• Closed—No connection state.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced

Related Commands

- `show ip interface` Displays the status and configuration of IP interfaces.
- `show tcp statistics` Displays TCP statistics.

MIB Objects

N/A
### show ip tcp half-open-timeout

Displays the timeout value configured for half-open TCP sessions.

```
show ip tcp half-open-timeout
```

---

#### Syntax Definitions

N/A

#### Defaults

N/A

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

N/A

#### Examples

```
-> show ip tcp half-open-timeout
Tcp Half-Open Timeout(Seconds): 15.
```

#### Release History

Release 8.4.1; command introduced

#### Related Commands

- `ip tcp half-open-timeout` Configures the timeout periods for dropping half-open TCP connections.

#### MIB Objects

- systemServicesTcpHalfOpenTimeout
show udp statistics

Displays UDP errors and statistics.

show udp statistics

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command displays cumulative statistics since the last time the switch was powered on or since the last reset of the switch.

Examples

-> show udp statistics

Total datagrams received = 214937,
Error datagrams received = 0,
No port datagrams received = 32891,
Total datagrams sent = 211884

output definitions

<table>
<thead>
<tr>
<th>Total datagrams received</th>
<th>Total number of UDP datagrams delivered to UDP applications.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error datagrams received</td>
<td>Number of UDP datagrams that could not be delivered for any reason.</td>
</tr>
<tr>
<td>No port datagrams received</td>
<td>Number of UDP datagrams that could not be delivered for reasons other than lack of application at the destination.</td>
</tr>
<tr>
<td>Total datagrams sent</td>
<td>Total number of UDP datagrams sent from this switch.</td>
</tr>
</tbody>
</table>

Release History
Release 7.1.1; command introduced
Related Commands

show udp ports
Displays the UDP Listener table.

MIB Objects

N/A
show udp ports

Displays the UDP Listener table. The table shows the local IP addresses and the local port number for each UDP listener.

show udp ports

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- An IP address of zero (0.0.0.0) indicates that it is listening on all interfaces.
- This table contains information about the UDP end-points on which a local application is currently accepting datagrams.

Examples

-> show udp ports

Local Address   Local Port
-------------+------------
0.0.0.0       67
0.0.0.0       161
0.0.0.0       520

output definitions

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Local Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local IP address for this UDP connection.</td>
<td>Local port number for this UDP connection.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced
Related Commands

show udp statistics Displays UDP errors and statistics.

MIB Objects

N/A
show ip dos config

Displays the DoS scan configuration for the switch.

show ip dos config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command allows the user to view the configuration parameters of the DoS scan. The scan keeps a record of the penalties incurred by certain types of packets on TCP and UDP ports. When the set penalty threshold is reached, it is assumed a DoS attack is in progress, and a trap is generated to inform the system administrator.

Examples

-> show ip dos config

<table>
<thead>
<tr>
<th>DoS type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>port scan</td>
<td>enabled</td>
</tr>
<tr>
<td>ping of death</td>
<td>enabled</td>
</tr>
<tr>
<td>loopback-src</td>
<td>enabled</td>
</tr>
<tr>
<td>invalid-ip</td>
<td>enabled</td>
</tr>
<tr>
<td>invalid-multicast</td>
<td>enabled</td>
</tr>
<tr>
<td>unicast dest-ip/multicast-mac</td>
<td>enabled</td>
</tr>
<tr>
<td>ping overload</td>
<td>disabled</td>
</tr>
<tr>
<td>arp flood</td>
<td>enabled</td>
</tr>
<tr>
<td>arp poison</td>
<td>enabled</td>
</tr>
<tr>
<td>anti-spoof</td>
<td>disabled</td>
</tr>
<tr>
<td>gratuitous-arp</td>
<td>disabled</td>
</tr>
<tr>
<td>ip-options-filter</td>
<td>enabled</td>
</tr>
<tr>
<td>DoS trap generation</td>
<td>= enabled,</td>
</tr>
<tr>
<td>DoS port scan threshold</td>
<td>= 1000,</td>
</tr>
<tr>
<td>DoS port scan decay</td>
<td>= 2,</td>
</tr>
</tbody>
</table>
DoS port scan close port penalty = 10,
DoS port scan TCP open port penalty = 0,
DoS port scan UDP open port penalty = 0,
Dos Maximum Ping Rate = 100
Dos Maximum ARP Request Rate = 500

output definitions

| DoS Type | The type of DoS attack. |
| Status | Whether or not detection for this type of DoS attack is enabled. Configured through the ip dos type command. |
| DoS trap generation | Displays the status of DoS trap generation. It is either ENABLED or DISABLED. Configured through the ip dos trap command. |
| DoS port scan threshold | The penalty threshold setting. When enough packets have increased the penalty number to this setting, a trap is generated to warn the administrator that a DoS attack is in progress. Configured through the ip dos scan threshold command. |
| DoS port scan decay | The decay value for the switch. The penalty value of the switch is decreased by this number every minute. Configured through the ip dos scan decay command. |
| DoS port scan close port penalty | The penalty value for packets received on closed UDP and TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on a closed UDP or TCP port. Configured through the ip dos scan close-port-penalty command. |
| DoS port scan TCP open port penalty | The penalty value for packets received on open TCP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open TCP port. Configured through the ip dos scan tcp open-port-penalty command. |
| DoS port scan UDP open port penalty | The penalty value for packets received on open UDP ports. The penalty number for the switch is increased by this amount every time a packet is received on an open UDP port. Configured through the ip dos scan udp open-port-penalty command. |

Release History

Release 7.1.1; command introduced
Release 8.7 R1; gratuitous-arp output field included.
Release 8.7 R2; ip-options-filter output field included.

Related Commands

- show ip dos statistics Displays the statistics for detected DoS attacks on the switch.
- ip dos type Enables or disables detection for the specified type of DoS attack.
MIB Objects

alaDosTable
   alaDoSType
   alaDoSStatus
alaDoSConfig
   alaDoSportScanClosePortPenalty
   alaDoSportScanUdpOpenPortPenalty
   alaDoSportScanTotalPenalty
   alaDoSportScanThreshold
   alaDoSportScanDecay
   alaDoSTrapCntl
   alaDoSARPRate
   alaDoSPingRate
show ip dos statistics

Displays the statistics for detected DoS attacks on the switch.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command displays the number of attacks the switch has detected for several types of DoS attacks.
- If an attack is detected and reported, it does not necessarily mean that an attack occurred. The switch assumes a DoS attack is underway anytime the penalty threshold is exceeded. It is possible for this threshold to be exceeded when no attack is in progress.
- Statistics for the “unicast dest-ip/multicast-mac” DoS type are not reported for the multicast MAC address attack. In this case, the packet is dropped at a lower level so IP never sees the attack. IP only collects and reports statistics for IP attacks.

Examples

-> show ip dos statistics

<table>
<thead>
<tr>
<th>DoS type</th>
<th>Attacks detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>port scan</td>
<td>0</td>
</tr>
<tr>
<td>ping of death</td>
<td>0</td>
</tr>
<tr>
<td>land</td>
<td>0</td>
</tr>
<tr>
<td>loopback-src</td>
<td>0</td>
</tr>
<tr>
<td>invalid-ip</td>
<td>0</td>
</tr>
<tr>
<td>invalid-multicast</td>
<td>0</td>
</tr>
<tr>
<td>unicast dest-ip/multicast-mac</td>
<td>52</td>
</tr>
<tr>
<td>ping overload</td>
<td>0</td>
</tr>
<tr>
<td>arp flood</td>
<td>0</td>
</tr>
<tr>
<td>arp poison</td>
<td>0</td>
</tr>
<tr>
<td>anti-spoof</td>
<td>0</td>
</tr>
<tr>
<td>gratuitous-arp</td>
<td>0</td>
</tr>
<tr>
<td>ip-options-filter</td>
<td>0</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS type</td>
<td>The type of DoS attack.</td>
</tr>
<tr>
<td>Attacks detected</td>
<td>The number of attacks detected for each DoS type.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced  
Release 8.7 R1; **gratuitous-arp** output field included.  
Release 8.7 R2; **ip-options-filter** output field included.

**Related Commands**

- **ip dos type**  
  Enables or disables detection for a specific type of DoS attack.
- **show ip dos config**  
  Displays the DoS scan configuration for the switch.

**MIB Objects**

- **alaDoSTable**
  - **alaDoSType**
  - **alaDoSDetected**
show vrf

Displays the Multiple VRF instance configuration for the switch.

`show vrf [vrf_name | default]`

**Syntax Definitions**

- `vrf_name` The name of an existing VRF instance.
- `default` Selects the default VRF instance.

**Defaults**

By default, a list of all VRF instances is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8</th>
<th>6900C32E/T24C2</th>
<th>6900X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `vrf_name` parameter to display route-map resource information for a specific VRF instance.
- Use the `default` parameter to display route-map resource information for the default VRF instance.
- The type of profile (low or max) assigned to a VRF determines the routing capabilities and the amount of route-map resources available for that specific VRF instance.

**Examples**

```
-> show vrf
  Virtual Routers    Profile Protocols
-------------------------------------------------
  default           default BGP PIM VRRP
  customer1         max   RIP OSPF
  customer2         max   RIP OSPF
  customer3         low

Total Number of Virtual Routers: 4
```

**output definitions**

- **Virtual Routers**: The name of the VRF instance.
- **Profile**: The type of profile applied to this instance (`low` or `max`).
- **Protocols**: The protocols loaded within the context of this instance.
-> show vrf customer1
Legend: in use/max
route-maps : 3/30,
sequences : 5/60,
vlvs : 8/100,
access-lists : 0/20,
address blocks : 0/40,
macth interfaces : 3/100

-> show vrf customer3
Legend: in use/max
route-maps : 0/10,
sequences : 0/20,
vlvs : 0/20,
access-lists : 0/10,
address blocks : 0/10,
macth interfaces : 0/10

-> show vrf default
Legend: in use/max
route-maps : 0/200,
sequences : 0/400,
vlvs : 0/1000,
access-lists : 0/200,
address blocks : 0/500,
macth interfaces : 0/2000

**output definitions**

- **route-maps**
  The number of route maps used and the maximum allowed.

- **sequences**
  The number of route map sequences used and the maximum allowed.

- **vlvs**
  The number of TLV blocks used and the maximum allowed. The TLV blocks contain the route-map match and set clauses.

- **access-lists**
  The number of route-map access lists used and the maximum allowed.

- **address blocks**
  The number of address blocks used and the maximum allowed. The address blocks hold access list addresses.

- **match interfaces**
  The number of route-map interfaces used in match clauses and the maximum allowed.

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.2; **Profile** field added, option to display route-map resources for a specific VRF instance.

**Related Commands**

- **vrf**
  Configures a Multiple VRF instance for the switch.

- **show vrf-profiles**
  Displays a summary of VRF profile usage and route map resources.

- **show ip protocols**
  Displays switch routing protocol information and status.
**MIB Objects**

alaVrConfigTable
   alaVrConfigIndex
   alaVrConfigRipStatus
   alaVrConfigOspfStatus
   alaVrConfigIsisStatus
   alaVrConfigBgpStatus
   alaVrConfigPimStatus
   alaVrConfigDvmrpStatus
   alaVrConfigRipngStatus
   alaVrConfigOspf3Status
   alaVrConfigMplsLdpStatus
   alaVrConfigVrrpStatus
alaVirtualRouterNameTable
   alaVirtualRouterName
   alaVirtualRouterNameIndex
   alaVirtualRouterNameRowStatus
   alaVirtualRouterProfile
   alaVirtualRouterMaxRouteMaps
   alaVirtualRouterMaxSequences
   alaVirtualRouterMaxTlvs
   alaVirtualRouterMaxAddressBlocks
   alaVirtualRouterMaxMatchInterfaces
**show vrf-profiles**

Displays the current VRF profile usage and the maximum route-map resources allowed for each profile type (default, low, and max).

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command also provides an estimate of the number of low profile VRFs that can be created.

**Examples**

```plaintext```
-> show vrf-profiles
EST: Estimated number of low profile VRFs that can be created
RM: Maximum route-maps
SEQ: Maximum sequences
TLV: Maximum TLVs (used to hold match and set clauses)
AL: Maximum access-lists
AB: Maximum address blocks (used to hold addresses)
ITF: Maximum route-map interfaces used in match clauses

<table>
<thead>
<tr>
<th>Profile</th>
<th>Inuse</th>
<th>EST</th>
<th>RM</th>
<th>SEQ</th>
<th>TLV</th>
<th>AL</th>
<th>AB</th>
<th>ITF</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>1</td>
<td>200</td>
<td>400</td>
<td>1000</td>
<td>200</td>
<td>500</td>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>low</td>
<td>2</td>
<td>329</td>
<td>10</td>
<td>20</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>max</td>
<td>3</td>
<td>30</td>
<td>60</td>
<td>100</td>
<td>20</td>
<td>40</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>
```

**Release History**

Release 7.3.2; command was introduced.
**Related Commands**

vrf
Configures and selects a VRF instance on the switch.

show vrf
Displays the VRF configuration for the switch.

**MIB Objects**

alaVirtualRouterProfileTable

alaVirtualRouterProfileName
alaVirtualRouterProfileMaxRouteMaps
alaVirtualRouterProfileMaxSequences
alaVirtualRouterProfileMaxTlvs
alaVirtualRouterProfileMaxAccessLists
alaVirtualRouterProfileMaxAddressBlocks
alaVirtualRouterProfileMaxMatchInterfaces
21 IPv6 Commands

This chapter details Internet Protocol Version 6 (IPv6) commands for the switch. IPv6 (documented in RFC 2460) is designed as a successor to IPv4. The changes from IPv4 to IPv6 fall primarily into the following categories:

**Expanded Routing and Addressing Capabilities** - IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy and a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses.

**Header Format Simplification** - Some IPv4 header fields were dropped or made optional, to reduce the common-case processing cost of packet handling and to keep the bandwidth cost of the IPv6 header as low as possible despite the increased size of the addresses. Even though the IPv6 addresses are four times longer than the IPv4 addresses, the IPv6 header is only twice the size of the IPv4 header.

**Anycast Addressing** - A new type of address called a "anycast address" is defined, to identify sets of nodes where a packet sent to an anycast address is delivered to one of the nodes. The use of anycast addresses in the IPv6 source route allows nodes to control the path on which their traffic flows.

**Improved Support for Options** - Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

**Authentication and Privacy Capabilities** - IPv6 includes the definition of extensions which provide support for authentication, data integrity, and confidentiality. This is included as a basic element of IPv6 and will be included in all implementations.

MIB information for the IPv6 and RIPng commands is as follows:

- **Filename**: IPV6-MIB.mib
  **Module**: Ipv6MIB

- **Filename**: ALCATEL-IND1-IPV6-MIB.mib
  **Module**: alcatelIND1Ipv6MIB

- **Filename**: ALCATEL-IND1-IPRMV6-MIB.mib
  **Module**: alcatelIND1IPRMV6MIB
A summary of the IPv6 commands is listed here:

<table>
<thead>
<tr>
<th>IPv6 Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 interface</code></td>
</tr>
<tr>
<td><code>ipv6 interface rtr-port</code></td>
</tr>
<tr>
<td><code>ipv6 interface tunnel source destination</code></td>
</tr>
<tr>
<td><code>ipv6 address</code></td>
</tr>
<tr>
<td><code>ipv6 address global-id</code></td>
</tr>
<tr>
<td><code>ipv6 address local-unicast</code></td>
</tr>
<tr>
<td><code>ipv6 dad-check</code></td>
</tr>
<tr>
<td><code>ipv6 hop-limit</code></td>
</tr>
<tr>
<td><code>ipv6 mtu-lifetime</code></td>
</tr>
<tr>
<td><code>ipv6 neighbor stale-lifetime</code></td>
</tr>
<tr>
<td><code>ipv6 neighbor</code></td>
</tr>
<tr>
<td><code>ipv6 neighbor limit</code></td>
</tr>
<tr>
<td><code>ipv6 neighbor vrf-limit</code></td>
</tr>
<tr>
<td><code>ipv6 ra-filter</code></td>
</tr>
<tr>
<td><code>ipv6 ra-filter trusted</code></td>
</tr>
<tr>
<td><code>ipv6 prefix</code></td>
</tr>
<tr>
<td><code>ipv6 static-route</code></td>
</tr>
<tr>
<td><code>ipv6 static-route all bfd-state</code></td>
</tr>
<tr>
<td><code>ipv6 static-route bfd-state</code></td>
</tr>
<tr>
<td><code>ipv6 route-pref</code></td>
</tr>
<tr>
<td><code>ipv6 virtual-source-mac</code></td>
</tr>
<tr>
<td><code>ipv6 echo</code></td>
</tr>
<tr>
<td><code>ipv6 icmp rate-limit</code></td>
</tr>
<tr>
<td><code>ping6</code></td>
</tr>
<tr>
<td><code>traceroute6</code></td>
</tr>
<tr>
<td><code>modify boot parameters</code></td>
</tr>
<tr>
<td><code>show ipv6 icmp statistics</code></td>
</tr>
<tr>
<td><code>show ipv6 interface</code></td>
</tr>
<tr>
<td><code>show ipv6 emp-interface</code></td>
</tr>
<tr>
<td><code>show ipv6 emp-routes</code></td>
</tr>
<tr>
<td><code>show ipv6 pmtu table</code></td>
</tr>
<tr>
<td><code>show ipv6 ra-filter</code></td>
</tr>
<tr>
<td><code>clear ipv6 neighbors</code></td>
</tr>
<tr>
<td><code>show ipv6 neighbors</code></td>
</tr>
<tr>
<td><code>show ipv6 prefixes</code></td>
</tr>
<tr>
<td><code>show ipv6 routes</code></td>
</tr>
<tr>
<td><code>show ipv6 route-pref</code></td>
</tr>
<tr>
<td><code>show ipv6 router database</code></td>
</tr>
<tr>
<td><code>show ipv6 tcp listeners</code></td>
</tr>
<tr>
<td><code>show ipv6 tcp connections</code></td>
</tr>
<tr>
<td><code>show ipv6 tunnel configured</code></td>
</tr>
<tr>
<td><code>show ipv6 tunnel 6to4</code></td>
</tr>
<tr>
<td><code>show ipv6 information</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv6 Route Map</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 redist</code></td>
</tr>
<tr>
<td><code>ipv6 access-list</code></td>
</tr>
<tr>
<td><code>ipv6 access-list address</code></td>
</tr>
<tr>
<td><code>show ipv6 redist</code></td>
</tr>
<tr>
<td><code>show ipv6 redist-routes</code></td>
</tr>
<tr>
<td><code>show ipv6 access-list</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Route Leak</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 export</code></td>
</tr>
<tr>
<td><code>ipv6 import</code></td>
</tr>
<tr>
<td><code>show ipv6 export</code></td>
</tr>
<tr>
<td><code>show ipv6 import</code></td>
</tr>
<tr>
<td><code>show ipv6 global-route-table</code></td>
</tr>
</tbody>
</table>
**ipv6 interface**

Configures an IPv6 VLAN, IPv6 tunnel, or Loopback0 interface.

```
ipv6 interface if_name [vlan vlan_id | service service_id | tunnel {tunnel_id | 6to4 | loopback0} admin-state [enable | disable] [base-reachable-time time] [ra-send {yes | no}] [ra-max-interval interval] [ra-managed-config-flag {true | false}] [ra-other-config-flag {true | false}] [ra-reachable-time time] [ra-retrans-timer time] [ra-default-lifetime time | no ra-default-lifetime] [ra-min-interval interval | no ra-min-interval] [ra-clock-skew time] [ra-preference {medium | low | high}] [ra-send-mtu] {yes | no} [ra-send-dnssl] {yes | no} [ra-send-rdns] {yes | no} [mtu size] [retrans-timer time] [dad-transmits count] [ra-hop-limit count] [[no] local-proxy-nd] [neighbor-limit count | no neighbor-limit] [retrans-backoff backoff] [retrans-max max]
```

```
no ipv6 interface if_name
```

### Syntax Definitions

- **if_name**  
  IPv6 interface name.
- **vlan_id**  
  VLAN ID number to identify a VLAN interface.
- **service_id**  
  An existing Shortest Path Bridging (SPB) service ID number (1–32767) to identify a service interface. *This parameter is supported only on the OmniSwitch 6860N, OmniSwitch 6900-X48C6/T48C6, OmniSwitch 6900-X48C4E, and OmniSwitch 9900.*
- **tunnel_id**  
  Tunnel ID number to identify a configured tunnel interface (not supported on the OmniSwitch 6465, OmniSwitch 6560 or the OmniSwitch 6570M).
- **6to4**  
  Identifies the 6to4 tunnel interface (not supported on the OmniSwitch 6465, OmniSwitch 6560 or the OmniSwitch 6570M).
- **loopback0**  
  Identifies a Loopback0 interface.
- **enable**  
  Administratively enable the interface.
disable

Administratively disable the interface.

base-reachable-time time

Base value used to compute the reachable time for neighbors reached through this interface.

ra-send {yes | no}

Specifies whether the router advertisements are sent on this interface.

ra-max-interval interval

Maximum time, in seconds, allowed between the transmission of unsolicited multicast router advertisements in this interface. The range is 4–1,800.

ra-managed-config-flag {true | false}

Value to be placed in the managed address configuration flag field in router advertisements sent on this interface.

ra-other-config-flag {true | false}

Value to be placed in the other stateful configuration flag in router advertisements sent on this interface.

ra-reachable-time time

Value, in milliseconds, to be placed in the reachable time field in router advertisements sent on this interface. The value zero indicates that the time is unspecified by the router.

ra-retrans-timer time

Value, in milliseconds, to be placed in the retransmit timer field in router advertisements sent on this interface. The value zero indicates that the time is unspecified by the router.

ra-default-lifetime time

Value, in seconds, to be placed in the router lifetime field in router advertisements sent on this interface. The time must be zero or between the value of ra-max-interval and 9,000 seconds. A value of zero indicates that the router is not to be used as a default router. The no ra-default-lifetime option will calculate the value using the formula (3 * ra-max-interval).

ra-min-interval interval

Value, in seconds, allowed between the transmission of unsolicited multicast router advertisements on this interface. The interval must be a minimum of 3 and not more than .75 times the value of ra-max-interval. The no ra-min-interval option will calculate the value using the formula (.33 * ra-max-interval).

ra-clock-skew time

Value, in seconds. The router advertisement clock skew allows the link propagation delays and poorly synchronized clocks on routers participating in router discover over this interface. The timer differences that fall within the clock skew value are treated as valid times.

ra-preference

Specify the router preference.

ra-send-mtu {yes | no}

Specifies whether the MTU option is included in the router advertisements sent on the interface.

ra-send-dnssl {yes | no}

Specifies whether the DNS Search List (DNSSL) option is included in the router advertisements sent on the interface.

ra-send-rdnss {yes | no}

Specifies whether the Recursive DNS Server (RDNSS) option is included in the router advertisements sent on the interface.

mtu size

The maximum transmission unit for a tunnel interface. Use the vlan command’s mtu-ip to set for a VLAN.

retrans-timer time

The amount of time, in milliseconds, between retransmission of a neighbor solicitation during neighbor discovery.

dad-transmits count

The number of neighbor solicitations to send during Duplicate Address Detection.
**ra-hop-limit** *count*

The value placed in the current hop limit field of router advertisements sent on this interface.

**[no]** local-proxy-nd

Enable or disable Local Proxy Neighbor Discovery (LPND) on the interface. The default value is no. **LPND can only be enabled on IPv6 VLAN interfaces and is not supported on the OmniSwitch 6465, OmniSwitch 6560 or the OmniSwitch 6570M.**

**neighbor-limit** *count*

Sets the neighbor cache limit for the interface. The range for this value is platform dependent:
- 16–64 on the OmniSwitch 6465.
- 16–128 on the OmniSwitch 6560 and OmniSwitch 6570M.
- 10–32000 on all other supported OmniSwitch platforms. If this value is not set, then no limit is enforced.

**no neighbor-limit**

Sets the neighbor cache limit back to the default value (64 for OmniSwitch 6465, 128 for OmniSwitch 6560 and OmniSwitch 6570M, and no limit is enforced for all other supported OmniSwitch platforms).

**retrans-backoff** *backoff*

Sets the Neighbor Unreachability Detection (NUD) exponential back-off base value. The configurable values are 1, 2 or 3. The default value is 1. This allows the exponentially increase of the interval between retransmissions of the Neighbor Solicitation (NS), providing a longer interval over which the neighbor can respond.

**retrans-max** *max*

Sets the maximum number of neighbor solicitations to be sent during ND and NUD. The range is from 1 to 10 with a default value of 3. This allows the number of neighbor solicitations sent for neighbor discovery to be increased.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-reachable-time</td>
<td>360</td>
</tr>
<tr>
<td>ra-send</td>
<td>yes</td>
</tr>
<tr>
<td>ra-max-interval</td>
<td>600</td>
</tr>
<tr>
<td>ra-managed-config-flag</td>
<td>false</td>
</tr>
<tr>
<td>ra-other-config-flag</td>
<td>false</td>
</tr>
<tr>
<td>ra-reachable-time</td>
<td>0</td>
</tr>
<tr>
<td>ra-retrans-time</td>
<td>0</td>
</tr>
<tr>
<td>ra-default-lifetime</td>
<td>calculated</td>
</tr>
<tr>
<td>ra-min-interval</td>
<td>calculated</td>
</tr>
<tr>
<td>ra-clock-skew</td>
<td>600</td>
</tr>
<tr>
<td>ra-preference</td>
<td>Medium</td>
</tr>
<tr>
<td>ra-send-mtu</td>
<td>no</td>
</tr>
<tr>
<td>ra-send-dnssl</td>
<td>no</td>
</tr>
<tr>
<td>ra-send-rdnss</td>
<td>no</td>
</tr>
<tr>
<td>retrans-timer</td>
<td>1000</td>
</tr>
<tr>
<td>dad-transmits</td>
<td>1</td>
</tr>
<tr>
<td>ra-hop-limit</td>
<td>64</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to delete an interface.
- When you create an IPv6 interface, it is enabled by default.
- All IPv6 VLAN, service, and tunnel interfaces must have a unique name.
- When creating an IPv6 interface for a VLAN, service, or a configured tunnel, specifying a VLAN ID, service ID, or a Tunnel ID is required. When modifying or deleting an interface, you do not need to specify one of these options unless the name assigned to the interface is being changed. If it is present with a different value from when the interface was created, the command will be in error.
- Specify the `service` parameter to create a service-based interface that is used to provide in-line routing for IPv6 over SPB. When creating an IPv6 interface for an SPB service, consider the following:
  - The SPB service ID specified must already exist in the switch configuration.
  - VLAN translation is automatically enabled when a service is assigned to an IPv6 interface regardless of whether or not VLAN translation is enabled for the service; the VLAN translation status is no longer configurable as long as the service is bound to an IPv6 interface.
  - When the last IPv6 interface is removed from a service, the VLAN translation status will return to its previous state. For example, if the administrative status was previously disabled, the status will revert to a disabled state when there are no more IP interfaces assigned to that service.
  - Mixing switches with VLAN translation enabled on some and disabled on other switches in the same network is not recommended. Make sure all switches have VLAN translation enabled, especially if a switch with a service-based interface is added to the network.
  - The same SPB service ID can be assigned to an IPv4 and an IPv6 interface as long as both interface types are in the same VRF instance.
  - See the “IP over SPBM” section in the “Configuring Shortest Path Bridging” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide for more information.
- A default 6to4 tunnel named “tunnel_6to4” is automatically created in the default VRF instance. The tunnel status and configuration can be changed, but the tunnel itself cannot be deleted.
- The 6to4 tunnel interface and the Loopback0 interface do not send router advertisements (`ra-send` is always set to `no`).

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-proxy-nd</td>
<td>no</td>
</tr>
<tr>
<td>retrans-backoff</td>
<td>1</td>
</tr>
<tr>
<td>retrans-max</td>
<td>3</td>
</tr>
</tbody>
</table>
Before a 6to4 tunnel or Loopback0 interface can be enabled, at least one address must be assigned to the interface.

To enable IPv6 routing you must first create a VLAN, then create an IPv6 interface on the VLAN. See Chapter 5, “VLAN Management Commands,” for information on creating VLANs.

To route IPv6 traffic over an IPv4 network, you must create an IPv6 tunnel using the `ipv6 interface` command.

Use the `no` option to disable the Local Proxy Neighbor Discovery on the interface.

Consistency checks are performed between the configured RA parameters and those present in received RAs. In the case of a discrepancy between the value in a received RA and the value configured on the switch, an informational message will be written to the SWLog log file. The messages are not logged on the console.

The `ra-managed-config-flag` and `ra-other-config flag` parameters specify the values to be present in RAs sent by the switch when the DHCPv6 server is disabled. If the DHCPv6 server is enabled, the M and O flags in RAs sent by the switch will always be true.

Before enabling the router advertisement option (MTU, DNSSL, and RDNSS) ensure the router advertisement (ra-send) is enabled on the switch.

**Examples**

```
-> ipv6 interface Test vlan 1
-> ipv6 interface Test_Tunnel tunnel 2
-> ipv6 interface Mgmt_intf loopback0
-> ipv6 interface vpn1 service 10
-> service 10 vlan-xlation disable
ERROR: Modify vlan translation currently not allowed for service (10)
-> ipv6 interface Test vlan 2 ra-send-dnssl yes
-> ipv6 interface Test vlan 2 ra-send-mtu yes ra-send-rdnss yes ra-send-dnssl yes
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; `loopback0` parameter added.
Release 8.7 R1; `ra-send-dnssl` and `ra-send-rdnss` parameter added.

**Related Commands**

- `show ipv6 interface`: Displays IPv6 Interface Table.
- `show ipv6 tunnel configured`: Displays IPv6 Configured Tunnel.
- `show ipv6 tunnel 6to4`: Displays IPv6 6to4 tunnel information.
- `show ipv6 information`: Displays IPv6 information.
**MIB Objects**

IPv6Ifindex
alaIPv6InterfaceTable
    alaIPv6InterfaceName
    alaIPv6InterfaceMtu
    alaIPv6InterfaceSendRouterAdvertisements
    alaIPv6InterfaceMaxRtrAdvInterval
    alaIPv6InterfaceAdvManagedFlag
    alaIPv6InterfaceAdvOtherConfigFlag
    alaIPv6InterfaceAdvRetransTimer
    alaIPv6InterfaceAdvDefaultLifetime
    alaIPv6InterfaceAdminStatus
    alaIPv6InterfaceAdvReachableTime
    alaIPv6InterfaceBaseReachableTime
    alaIPv6InterfaceAdvSendMtu
    alaIPv6InterfaceAdvSendRDNSS
    alaIPv6InterfaceAdvSendDNSSL
    alaIPv6InterfaceLPND
    alaIPv6InterfaceNeighborLimit
    alaIPv6InterfaceRetransBackoff
    alaIPv6InterfaceRetransMax
**ipv6 interface rtr-port**

Configures an IPv6 routed-port interface by associating an IPv6 interface with a port or link aggregate and a VLAN.

```
ipv6 interface if_name rtr-port {port chassis/slot/port | linkagg agg_id} {tagged | untagged} vlan vlan_id
```

**Syntax Definitions**

- `if_name` A unique name for the IPv6 interface. Use quotes around the string if the name contains multiple words with spaces between them (for example, “ALE Marketing”). This value is case sensitive.
- `chassis/slot/port` The chassis, slot, and port number (1/2/1) of the physical port to bind to the IPv6 interface.
- `agg_id` The link aggregate ID to bind to the IP Interface.
- `tagged` Whether the assigned port or link aggregate is tagged for the specified VLAN.
- `untagged` Whether the assigned port or link aggregate is untagged for the specified VLAN.
- `vlan_id` An unused VLAN ID to which this IPv6 interface is associated.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- In a single step, this command creates the specified VLAN, configures an IPv6 interface for the VLAN, and assigns a port or link aggregate (tagged or untagged) to the VLAN. The `ipv6 address` command is then used to assign and IPv6 address to the routed-port interface.

- Configuring an IPv4 and IPv6 routed-port interface for the same VLAN ID is supported if the following conditions are met:
  - The VLAN ID, port, and the tagged/untagged port status for both interfaces is the same (for example, IPv4 and IPv6 routed interfaces are both bound to VLAN 850 with port 1/1/2 tagged).
  - Both interfaces are configured in the same VRF instance.
• Make sure the specified VLAN ID does not already exist in the switch configuration or is only used as a routed-port VLAN for an IPv4 interface. This VLAN will serve as a routing-only VLAN with a single port or link aggregate (Layer 2 functionality is not supported).

• Make sure the specified port or link aggregate is not already assigned to a VLAN that is not a routed-port VLAN. However, the port or link aggregate can be assigned to other routed-port VLANs.

• Attempting to add more ports or link aggregates to the routed-port VLAN or attempting to delete the VLAN is not allowed. The VLAN can only be removed by deleting the associated IPv6 and, if configured, the associated IPv4 interface.

• The same VLAN cannot be used for both a routed-port interface and a non-routed port interface.

• Once configured, an IPv6 routed port interface is operationally equivalent to an IPv6 VLAN interface. Routing protocols and other switch features that use IPv6 are configured and operate on an IPv6 routed port interface in the same manner as on a regular IPv6 interface.

**Examples**

`-> ipv6 interface rp-vlan30 rtr-port port 1/1/1 tagged vlan 30`

`-> ipv6 interface rp-vlan40 rtr-port port 1/1/2 untagged vlan 40`

`-> ipv6 interface rp-vlan50 rtr-port linkagg 6 tagged vlan 50`

`-> ipv6 interface rp-vlan60 rtr-port linkagg 7 untagged vlan 60`

`-> ipv6 interface rp-vlan50 rtr-port port 1/1/3 untagged vlan 60`

**ERROR:** Routed port interface rp-vlan60 VLAN and/or port configuration cannot be changed

`-> no ipv6 interface rp-vlan60`

`-> vlan 70`

`-> ipv6 interface rp-vlan70 rtr-port port 1/1/15 untagged vlan 70`

**ERROR:** VLAN 70 already exists

`-> ip interface rpv4-port rtr-port port 1/1/2 tagged vlan 850`

`-> ipv6 interface rpv6-port rtr-port port 1/1/2 tagged vlan 850`

`-> no ipv6 interface rpv6-port`

`-> ipv6 interface rpv6-port rtr-port port 1/1/2 untagged vlan 850`

**ERROR:** Configuration conflict with IPv4 routed port interface rp-port

**Release History**

Release 8.6R2; command introduced

**Related Commands**

- `show ipv6 interface` Displays the status and configuration of IPv6 interfaces.

**MIB Objects**

- `alaIPv6InterfaceTable`
  - `alaIPv6InterfaceName`
  - `alaIPv6InterfaceRoutedPortIfIndex`
  - `alaIPv6InterfaceRoutedPortTag`
ipv6 interface tunnel source destination

Configures the source and destination IPv4 addresses for a configured tunnel.

```
ipv6 interface if_name tunnel {source ipv4_source destination ipv4_destination}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if_name</code></td>
<td>Name assigned to the tunnel interface.</td>
</tr>
<tr>
<td><code>ipv4_source</code></td>
<td>Source IPv4 address for the configured tunnel.</td>
</tr>
<tr>
<td><code>ipv4_destination</code></td>
<td>Destination IPv4 address for the configured tunnel.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `ipv6 interface` command to create an IPv6 tunnel interface.
- A configured tunnel interface cannot be enabled until both its IPv4 source and destination addresses have been specified.

### Examples

```
-> ipv6 interface Test tunnel 2 source 192.0.2.1 destination 198.51.100.1
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `ipv6 interface`: Creates an IPv6 tunnel interface.
- `show ipv6 tunnel configured`: Displays IPv6 tunnel information.

### MIB Objects

- **IPv6IfIndex**
  - `alaIPv6ConfigTunnelv4Source`
  - `alaIPv6ConfigTunnelv4Dest`
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaIPv6ConfigTunnelRowStatus</td>
<td></td>
</tr>
</tbody>
</table>
**ipv6 address**

Configures an IPv6 address for an IPv6 interface. There are different formats for this command depending on the address type.

```
ipv6 address ipv6_address/prefix_length {if_name | loopback}
```

```
no ipv6 address ipv6_address {if_name | loopback}
```

```
ipv6 address ipv6_prefix eui-64 {if_name | loopback}
```

```
no ipv6 address ipv6_prefix eui-64 {if_name | loopback}
```

**Syntax Definitions**

- `ipv6_address` IPv6 address.
- `/prefix_length` The number of bits that are significant in the IPv6 address (mask). (3..128).
- `eui-64` Append an EUI-64 identifier to the prefix.
- `if_name` Name assigned to the interface.
- `loopback` Configures an IPv6 address for the loopback interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete an address.
- You can assign multiple IPv6 addresses to an IPv6 interface.
- No default value for prefix length. However, the prefix for the loopback or the user-defined Loopback0 interface must always be /128.
- Make sure that only 6to4 addresses are assigned to a 6to4 tunnel interface.
- The “eui” form of the command is used to add or remove an IPv6 address for a VLAN or configured tunnel using an EUI-64 interface ID in the low order 64 bits of the address.
- When JITC mode is enabled, Site-Local addresses of range FEC0::/10 cannot be configured. This consists of all the addresses that begin with FEC, FED, FEE, and FEF. Refer to the “AAA Commands”
chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide* for more information on enabling JITC mode.

**Examples**

-> ipv6 address 2001:db8:4132:86::19a/64 Test_Lab
-> ipv6 address 2002:c633:6489::35/64 Test_6to4
-> ipv6 address 2001:db8:6489::36/128 loopback
-> ipv6 interface Test_Loopback0 loopback0
-> ipv6 address 2001:db8:6489::37/128 Test_Loopback0

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1: *anycast* keyword deprecated.

**Related Commands**

*show ipv6 interface* Displays IPv6 Interface Table.

**MIB Objects**

IPv6IfIndex
alaIPv6InterfaceAddressTable
  alaIPv6InterfaceAddress
    alaIPv6InterfaceEUI64AddressPrefixLength
    alaIPv6InterfaceEUI64AddressRowStatus

For EUI-64 Addresses:
alaIPv6InterfaceEUI64AddressesTable
  alaIPv6InterfaceEUI64Address
  alaIPv6InterfaceEUI64AddressPrefixLength
  alaIPv6InterfaceEUI64AddressRowStatus
### ipv6 address global-id

Automatically generates or allows a new global ID to be entered.

```
ipv6 address global-id {generate | globalID}
```

#### Syntax Definitions

- **generate**: Automatically generates the global ID.
- **globalID**: A 5-byte global ID value specified in the form hh:hh:hh:hh:hh

#### Defaults

By default, the IPv6 global ID is set to all zeros.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- Global ID needs to be automatically generated or configured explicitly.
- A 40-bit global identifier is used to make the local IPv6 address prefixes globally unique.
- The global ID will be generated the first time a local unicast address is added through the `ipv6 address local-unicast` command or when the `ipv6 address global-id` command is executed.

#### Examples

- `ipv6 address global-id generate`
- `ipv6 address global-id 32:57a3:8fed`

#### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ipv6 address local-unicast` Creates a IPv6 local unicast address using the configured global ID.
- `ipv6 bgp unicast` Enables or disables unicast IPv6 updates for the BGP routing process.
- `show ip bgp` Displays the current global settings for the local BGP speaker.

**MIB Objects**

- `alaIPv6GlobalID`
**ipv6 address local-unicast**

Creates a IPv6 local unicast address using the configured global ID.

```
ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] [interface-id interfaceID | eui-64] [prefix-length prefixLength] {if_name | loopback}
```

```
no ipv6 address local-unicast [global-id globalID] [subnet-id subnetID] [interface-id interfaceID | eui-64] [prefix-length prefixLength] {if_name | loopback}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>globalID</td>
<td>A 5-byte global ID value specified in the form hh:hhhh:hhhh.</td>
</tr>
<tr>
<td>subnetID</td>
<td>A 2-byte Subnet ID specified in the form 0xhhhh. The valid range is 0x0000-0xffff or 0-65535.</td>
</tr>
<tr>
<td>eui-64</td>
<td>Automatically-generated EUI-64 value to be used for interface identifier.</td>
</tr>
<tr>
<td>prefixLength</td>
<td>The number of bits that are significant in the IPv6 address (mask). The valid range is 0-128; however, the default value must rarely be overridden.</td>
</tr>
<tr>
<td>if_name</td>
<td>The name assigned to the interface.</td>
</tr>
<tr>
<td>loopback</td>
<td>The loopback for the loopback interface.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefixLength</td>
<td>64</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the local unicast address. However, addresses are normally deleted using the `ipv6 address` command.
- If the global ID value is not explicitly specified, the default global ID set by the `ipv6 address global-id` command is used.
- If the global ID value is explicitly configured using the `ipv6 address local-unicast` command, the address’ global ID will not be changed if the `ipv6 address global-id` command is executed.
The use of a double-colon abbreviation for the interface identifier, similar to that used for full IPv6 addresses, is allowed.

**Examples**

```
-> ipv6 address local-unicast global-id 0073:110:255 subnet-id 23 interface-id 215:60ff:fe7a:adc0 prefix-length 64 loopback
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ipv6 address global-id` Automatically generates or allows a new global ID to be entered.
- `show ipv6 information` Displays IPv6 information.

**MIB Objects**

- `alaIPv6LocalUnicastGlobalID`
- `alaIPv6LocalUnicastSubnetID`
- `alaIPv6LocalUnicastInterfaceID`
- `alaIPv6LocalUnicastEUI64`
- `alaIPv6LocalUnicastPrefixLength`
ipv6 dad-check

Runs a Duplicate Address Detection (DAD) check on an address that was marked as duplicated.

ipv6 dad-check ipv6_address if_name

**Syntax Definitions**

- *ipv6_address* IPv6 address.
- *if_name* Name assigned to the interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The switch performs DAD check when an interface is attached and its VLAN first enters the active state. Use this command to rerun a DAD check on an address that was marked as duplicated.

**Examples**

- `-> ipv6 dad-check 2001:db8::1/32 Test_Lab`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

N/A

**MIB Objects**

alaIPv6InterfaceAddressTable
  - alaIPv6InterfaceAddressDADStatus
ipv6 hop-limit

Configures the value placed in the hop limit field in the header of all IPv6 packets that are originated by the switch. It also configures the value placed in the hop limit field in router advertisements.

ipv6 hop-limit value

no ipv6 hop-limit

Syntax Definitions

value Hop limit value. The range is 0 - 255.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>64</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to return the hop limit to its default value.
- Inputting the value 0 (zero) will result in the default (64) hop-limit.

Examples

-> ipv6 hop-limit 64

Release History

Release 7.1.1; command was introduced.
Related Commands

show ipv6 information Displays IPv6 information.

MIB Objects

ipv6MibObjects
  Ipv6DefaultHopLimit
ipv6 pmtu-lifetime

Configures the minimum lifetime for entries in the path MTU Table.

*ipv6 pmtu-lifetime* *time*

---

**Syntax Definitions**

*time* Minimum path MTU entry lifetime, in minutes. Valid range is 10–1440.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>10</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

`-> ipv6 pmtu-lifetime 30`

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- *show ipv6 pmtu table* Displays the IPv6 path MTU Table.
- *show ipv6 information* Displays IPv6 information.

---

**MIB Objects**

- *alaIPv6ConfigTable*
  - *alaIPv6PMTUMinLifetime*
**ipv6 neighbor stale-lifetime**

Configures the minimum lifetime for neighbors in the unconfirmed state.

**ipv6 neighbor stale-lifetime**

---

**Syntax Definitions**

- **stale-lifetime**: Minimum lifetime for neighbor entries in the stale state (5–2800).

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>stale-lifetime</td>
<td>10</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

```
-> ipv6 neighbor stale-lifetime 1400
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `show ipv6 neighbors` Displays IPv6 Neighbor Table.
- `show ipv6 information` Displays IPv6 information.

---

**MIB Objects**

- `IPv6IfIndex`
- `alaIPv6NeighborTable` `alaIPv6NeighborStaleLifetime`
**ipv6 neighbor**

Configures a static entry in the IPv6 Neighbor Table.

```
ipv6 neighbor ipv6_address hardware_address {if_name} {port chassis/slot/port | linkagg agg_id}
no ipv6 neighbor ipv6_address {if_name}
```

### Syntax Definitions

- **ipv6_address**: IPv6 address that corresponds to the hardware address.
- **hardware_address**: MAC address in hex format (e.g., 00:00:39:59:F1:0C).
- **if_name**: Name assigned to the interface on which the neighbor resides.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number of the port used to reach the neighbor.
- **agg_id**: The link aggregate ID number of the link aggregate used to reach the neighbor.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `no` form of this command to remove an entry from IPv6 Neighbor Table.

### Examples

```
-> ipv6 neighbor 4132:86::203 00:d0:c0:86:12:07 Test port 1/1
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 neighbors* Displays IPv6 Neighbor Table.

**MIB Objects**

IPv6IfIndex
alaIPv6NeighborTable
  alaIPv6NeighborNetAddress
  alaIPv6NeighborPhysAddress
  alaIPv6NeighborSlot
  alaIPv6NeighborPort
  alaIPv6NeighborRowStatus
  alaIPv6NeighborStaleLifetime
**ipv6 neighbor limit**

Configures the system-wide maximum limit for the number of neighbor entries in the cache.

**ipv6 neighbor limit** *count*

no ipv6 neighbor limit

---

**Syntax Definitions**

- **count**
  
  The system-wide maximum limit for the number of neighbor entries in the cache. The valid range for this value is platform dependent:
  
  - 16–64 on the OmniSwitch 6465.
  - 16–128 on the OmniSwitch 6560 and OmniSwitch 6570M.
  - 200–32000 on all other supported OmniSwitch platforms. If this value is not set, then no limit is enforced.

---

**Defaults**

By default, the maximum number of neighbor entries is set to 64 on the OmniSwitch 6465 and 128 on the OmniSwitch 6560 and OmniSwitch 6570M. On all other supported OmniSwitch platforms, there is no enforced limit.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the no form of this command to set the limit back to the default value.

---

**Examples**

- -> ipv6 neighbor limit 16
- -> ipv6 neighbor limit 200
- -> no ipv6 neighbor limit

---

**Release History**

Release 8.1.1; command introduced.
Related Commands

ipv6 interface
Creates an IPv6 tunnel interface.

show ipv6 information
Displays IPv6 information.

MIB Objects

alaIPv6NeighborTable
alaIPv6NeighborLimit
**ipv6 neighbor vrf-limit**

Configures the maximum limit for the number of neighbor entries in a VRF's cache.

**ipv6 neighbor vrf-limit count**

**no ipv6 neighbor vrf-limit**

---

**Syntax Definitions**

`count` The maximum limit for the number of VRF neighbor entries in the cache. The valid range for this value is platform dependent:
- 16–64 on the OmniSwitch 6465.
- 16–128 on the OmniSwitch 6560.
- 200–32000 on all other supported OmniSwitch platforms. If this value is not set, then no limit is enforced.

---

**Defaults**

By default, the maximum number of neighbor entries is set to 64 on the OmniSwitch 6465 and 128 on the OmniSwitch 6560. On all other supported OmniSwitch platforms, there is no enforced limit.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the `no` form of this command to set the limit back to the default value.

---

**Examples**

- `-> ipv6 neighbor vrf-limit 16`
- `-> ipv6 neighbor vrf-limit 200`
- `-> no ipv6 neighbor vrf-limit`

---

**Release History**

Release 8.1.1; command introduced.
Related Commands

ipv6 interface  Creates an IPv6 tunnel interface.
show ipv6 information  Displays IPv6 information.

MIB Objects

alaIPv6NeighborTable
  alaIPv6NeighborVRFLimit
**ipv6 ra-filter**

Configures the status of Router Advertisement (RA) filtering on IPv6 VLAN interfaces. When RA filtering is enabled on an interface, RAs received on any port or linkagg will be discarded. If one or more trusted ports or link aggregates are configured, RAs received on them will be accepted and sent on to any connected IPv6 nodes.

```
ipv6 ra-filter if-name [admin-state {enable | disable}]
no ipv6 ra-filter if-name
```

**Syntax Definitions**

- **if-name** Specify the name of the IPv6 VLAN interface.
- **enable** Enables RA filtering on the specified interface.
- **disable** Disables RA filtering on the specified interface.

**Defaults**

By default, the administrative status of RA filtering on an IPv6 VLAN interface is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to return the RA filtering status to the default value (disabled).

**Examples**

```
-> ipv6 ra-filter vlan-23 admin-state enable
-> ipv6 ra-filter vlan-23 admin-state disable
-> no ipv6 ra-filter vlan-23
```

**Release History**

Release 8.1.1; command introduced.
Release 8.5R2; OmniSwitch 6560 support for IPv6 RA Filtering added.
**Related Commands**

- **ipv6 ra-filter trusted**
  - Configures trusted ports or link aggregates on which RAs are accepted when RA filtering is enabled.

- **ipv6 interface**
  - Creates an IPv6 interface.

- **show ipv6 interface**
  - Displays IPv6 Interface Table.

- **show ipv6 ra-filter**
  - Displays the RA filter configuration for an IPv6 interface.

**MIB Objects**

- **alaIPv6RAFilterInterfaceTable**
  - **alaIPv6RAFilterInterfaceAdminStatus**
  - **alaIPv6RAFilterInterfaceRowStatus**
**ipv6 ra-filter trusted**

Configures trusted sources (ports or link aggregates) on which Router Advertisements (RAs) are accepted and sent on to any connected IPv6 nodes. When RA filtering is enabled on an IPv6 VLAN interface, RAs received on any port or linkagg will be discarded, except on trusted ports or link aggregates.

**ipv6 ra-filter** if-name trusted {port chassis/slot/port | linkagg agg_id}

**no ipv6 ra-filter** if-name trusted {port chassis/slot/port | linkagg agg_id}

---

**Syntax Definitions**

- **if-name** Specify the name of the IPv6 VLAN interface on which RA filtering is enabled or disabled.
- **chassis/slot/port** The chassis ID, slot, and port number (3/1/1) for a trusted port.
- **agg_id** A trusted link aggregate ID number.

**Defaults**

By default all ports and link aggregates are untrusted.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to return a port or linkagg to an untrusted state.
- Use the **ipv6 ra-filter** command to enable or disable the RA filtering status for an IPv6 VLAN interface.

**Examples**

- `-> ipv6 ra-filter vlan-23 trusted port 1/1/22`
- `-> ipv6 ra-filter vlan-23 trusted linkagg 10`
- `-> no ipv6 ra-filter vlan-23 trusted port 1/1/22`
- `-> no ipv6 ra-filter vlan-23 trusted linkagg 10`

**Release History**

Release 8.1.1; command introduced.
Release 8.5R2; OmniSwitch 6560 support for IPv6 RA Filtering added.
Related Commands

- `ipv6 ra-filter`: Configures the RA filtering status for an IPv6 VLAN interface.
- `ipv6 interface`: Creates an IPv6 tunnel interface.
- `show ipv6 interface`: Displays IPv6 Interface Table.
- `show ipv6 ra-filter`: Displays the RA filter configuration for an IPv6 interface.

MIB Objects

- `alaIPv6RAFilterTrustedSourceTable`  
- `alaIPv6RAFilterTrustedSourceRowStatus`
**ipv6 prefix**

Configures an IPv6 prefix on an interface. Used for configuring prefixes for router advertisements.

```
ipv6 prefix ipv6_address /prefix_length if_name [valid-lifetime time] [preferred-lifetime time] [on-link-flag {true | false} [autonomous-flag {true | false}]] if_name
```

```
no ipv6 prefix ipv6_address /prefix_length if_name
```

**Syntax Definitions**

- **ipv6_address**: IPv6 address of the interface.
- **/prefix_length**: The number of bits that are significant in the IPv6 address (mask). (1...127).
- **valid-lifetime time**: Length of time, in seconds, that this prefix will remain valid (i.e. time until deprecation). A value of 4,294,967,295 represents infinity.
- **preferred-lifetime time**: Length of time, in seconds, that this prefix will remain preferred (i.e. time until deprecation). A value of 4,294,967,295 represents infinity.
- **on-link-flag {true | false}**: On-link configuration flag. When “true” this prefix can be used for on-link determination.
- **autonomous-flag {true | false}**: Autonomous address configuration flag. When “true”, indicates that this prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).
- **if_name**: Name assigned to the interface.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>valid-lifetime time</td>
<td>2,592,000</td>
</tr>
<tr>
<td>preferred-lifetime time</td>
<td>604,800</td>
</tr>
<tr>
<td>on-link-flag</td>
<td>true</td>
</tr>
<tr>
<td>autonomous-flag</td>
<td>true</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **no** form of this command to delete a prefix.
Examples

-> ipv6 prefix 4132:86::/64 Test

Release History

Release 7.1.1; command was introduced.

Related Commands

- show ipv6 prefixes
  Displays IPv6 prefixes used in router advertisements.

MIB Objects

IPv6IfIndex
alaIPv6InterfacePrefixTable
  allaIPv6vInterfacePrefix
  allaIPv6vInterfacePrefixLength
  allaIPv6vInterfacePrefixValidLifetime
  allaIPv6vInterfacePrefixPreferredLifetime
  allaIPv6vInterfacePrefixonLinkFlag
  allaIPv6vInterfacePrefixAutonomousFlag
  allaIPv6vInterfacePrefixRowStatus
**ipv6 static-route**

Configures an IPv6 static route. Static routes are user-defined; they carry a higher priority than routes created by dynamic routing protocols. By default, static routes carry a higher priority than dynamic routes.

```
ipv6 static-route ipv6_prefix/prefix_length gateway {ipv6_address | null} [tag num] [name string] [if_name] [emp] [metric metric]
```

```
no ipv6 static-route ipv6_prefix/prefix_length gateway {ipv6_address | null} [if_name] [emp]
```

**Syntax Definitions**

- `ipv6_prefix` IPv6 network that is the destination of this static route.
- `/prefix_length` The number of bits (0...128) that are significant in the IPv6 address (mask).
- `gateway ipv6_address` IPv6 address of the next hop used to reach the destination IPv6 address.
- `gateway null` Use this option to configure an IPv6 blackhole route.
- `num` Tag to be used for route.
- `string` Name to be used for route.
- `if_name` If the next hop is a link-local address, the name of the interface used to reach it.
- `emp` Represents the EMP interface.
- `metric` Metric or cost (hop count) for the static route. You can set a priority for the static route by assigning a metric value. The lower the metric value, the higher the priority. Valid range is 1–15.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

|       | 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 V72/C32 | 6900 X48C6/T48C6 | X48C4E/V48C8/C32E/T24C2 | X24C2 | 9900 |
|-------|------|------|------|-------|------|-------|------|------|-------------|------------------|----------------|$ | |
|       | Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes          | Yes              | Yes             | Yes             |

**Usage Guidelines**

- Use the `no` form of this command to remove a static route.
- By default, static routes have a higher priority over dynamic routes; however, it can be changed using the `ipv6 route-pref` command.
• To create an IPv6 static route with gateway pointing to an EMP interface, specify the keyword `emp` for the interface name field instead of specifying the exact interface name of the EMP interface (for example, EMP-CMMA-CHAS1).

• If IPv6 address is configured on the EMP port on a VC or chassis setup, ensure to configure the IPv6 address on all the VC elements or CMM.

• Static route with default gateway towards EMP interface is not allowed.

• Use the `null` option to configure IPv6 blackhole routes. A blackhole route is used to forward unwanted traffic to a blackhole.
  
  – Redistribution of blackhole routes is supported. Dynamic routing protocols may advertise these routes, but the gateway associated with the route(s) will be an address on the router advertising them.
  
  – Leaking of blackhole routes across SPB service backbones is supported. However, blackhole routes cannot be leaked between VRFs. Blackhole routes need to be explicitly configured using the `ip static-route` command in any/all VRFs.
  
  – Blackhole routes are created and installed through static route commands. Dynamic Routing protocols shall not install blackhole IPv6 routes.
  
  – Blackhole routes shall never be part of ECMP.
  
  – Blackhole routes cannot be enabled for BFD support.

• Alternatively, the gateway address `::` can be used to create an IPv6 blackhole route.

**Examples**

-> ipv6 static-route 212:95:5::/64 gateway fe80::2d0:95ff:fe6a:f458 v6if-137 metric 3

Static route with gateway towards EMP interface:

-> ipv6 static-route 212:95:5::/64 gateway 2001::205 emp

or

-> ipv6 static-route 212:95:5::/64 gateway 2001::205 EMP-CMMA-CHAS1

Static route with default gateway towards EMP interface is not allowed.

-> ipv6 static-route ::/0 gateway 2001::205 EMP-CMMA-CHAS1

ERROR: Default routes with gateway on EMP port not allowed

Configuring a static blackhole route.

-> ipv6 static-route 212:95:5::/64 gateway null

-> ipv6 static-route 22::/64 gateway ::

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; `tag` and `name` parameters included.
Release 8.4.1; `emp` parameter added.
Release 8.6R1; `null` keyword added.
**Related Commands**

- **modify boot parameters**
  This command is used to configure IPv6 EMP interface.

- **show ipv6 routes**
  Displays IPv6 Forwarding Table.

- **show ipv6 router database**
  Displays a list of all routes (static and dynamic) that exist in the IPv6 router database.

- **show ipv6 route-pref**
  Displays the IPv6 routing preference of the router.

**MIB Objects**

- `alaIprmv6StaticRouteTable`
  - `alaIprmv6StaticRouteDest`
  - `alaIprmv6StaticRoutePrefixLength`
  - `alaIprmv6StaticRouteNextHop`
  - `alaIprmv6StaticRouteTag`
  - `alaIprmv6StaticRoute_Name`
  - `alaIprmv6StaticRouteIfIndex`
  - `alaIprmv6StaticRouteMetric`
  - `alaIprmv6StaticRouteRowStatus`
**ipv6 static-route all bfd-state**

Enables BFD for all IPv6 static routes.

```bash
disable enable
```

**Syntax Definitions**

- `enable`: Enables BFD for all IPv6 static routes.
- `disable`: Disables BFD for all IPv6 static routes.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When there are static routes configured in the switch, BFD is enabled to track the gateway.
- If the route is not reachable, it will be moved to the inactive database.

**Examples**

```bash
-> ipv6 static-route all bfd-state enable
-> ipv6 static-route all bfd-state disable
```

**Release History**

Release 8.4.1.R03; command was introduced.

**Related Commands**

- `ipv6 static-route bfd-state`: Enables BFD for a specific static route.
- `show ipv6 router database`: Displays a list of all routes (static and dynamic) that exist in the IP router database.

**MIB Objects**

- `alaIprmV6Config`
- `alaIprmV6StaticAllBfd`
**ipv6 static-route bfd-state**

Enables or disables BFD for a specific IPv6 static route.

`ipv6 static-route ipv6_prefix/pfx_length gateway ipv6_host_address bfd-state {enable| disable}`

### Syntax Definitions

- `ipv6_prefix` The destination IPv6 address.
- `pfx_length` The prefix length for the destination IPv6 address.
- `ipv6_host_address` The gateway IPv6 address.
- `enable` Enables BFD for the IPv6 static route.
- `disable` Disables BFD for the IPv6 static route.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

BFD is enabled to track the gateway of static routes.

### Examples

```
-> ipv6 static-route 195:35::/64 gateway fe80::2d0:95ff:fe12:f470 bfd-state enable
-> ipv6 static-route 195:35::/64 gateway fe80::2d0:95ff:fe12:f470 bfd-state disable
```

### Release History

Release 8.4.1.R03; command was introduced.

### Related Commands

- `ipv6 static-route all bfd-state` Enables BFD for all static routes.
- `show ipv6 router database` Displays a list of all routes (static and dynamic).
### MIB Objects

- `alaIprmV6StaticRouteTable`
- `alaIprmV6StaticRouteDest`
- `alaIprmV6StaticRoutePfxLength`
- `alaIprmV6StaticRouteNextHop`
- `alaIprmV6StaticRouteIfIndex`
- `alaIprmV6StaticRouteBfdStatus`
- `alaIprmV6StaticRouteType`
**ipv6 route-pref**

Configures the route preference of a router.

```
ipv6 route-pref {static | ospf | rip | ebgp | ibgp | isisl1 | isisl2 | import} value
```

### Syntax Definitions

- **static**
  - Configures the route preference of static routes.

- **ospf**
  - Configures the route preference of OSPF3 routes. *(OSPF3 is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M).*

- **rip**
  - Configures the route preference of RIPng routes.

- **ebgp**
  - Configures the route preference of external BGP routes. *(the IPv6 version of BGP is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M).*

- **ibgp**
  - Configures the route preference of internal BGP routes. *(the IPv6 version of BGP is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M).*

- **isisl1**
  - Configures the route preference of IS-IS L1 routes. *(IS-IS is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M or OmniSwitch 9900).*

- **isisl2**
  - Configures the route preference of IS-IS L2 routes. *(IS-IS is not supported on the OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6570M or OmniSwitch 9900).*

- **import**
  - Configures the route preference for the routes that are imported from another VRF instance.

- **value**
  - Route preference value. The valid range is 1–255.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>static value</td>
<td>2</td>
</tr>
<tr>
<td>ospf value</td>
<td>110</td>
</tr>
<tr>
<td>rip value</td>
<td>120</td>
</tr>
<tr>
<td>ebgp value</td>
<td>190</td>
</tr>
<tr>
<td>ibgp value</td>
<td>200</td>
</tr>
<tr>
<td>isisl1 value</td>
<td>115</td>
</tr>
<tr>
<td>isisl2 value</td>
<td>118</td>
</tr>
<tr>
<td>import value</td>
<td>210</td>
</tr>
</tbody>
</table>
**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Route preference of local routes cannot be changed.

**Examples**

- `-> ipv6 route-pref ospf 20`
- `-> ipv6 route-pref rip 60`

**Release History**

Release 7.1.1; command was introduced.  
Release 8.5R1; `import` parameter added.

**Related Commands**

`show ipv6 route-pref`  
Displays the configured route preference of a router.

**MIB Objects**

- `alaIprmV6RtPrefTable`
- `alaIprmV6RtPrefEntryType`
- `alaIprmV6RtPrefEntryValue`
**ipv6 virtual-source-mac**

Configures the source MAC to be used for packets being sent from a VRRP instance.

```
ipv6 virtual-source-mac {on | off}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtual-source-mac</td>
<td>off</td>
</tr>
</tbody>
</table>

#### on

The switch will use the VRRP virtual MAC address for all packets.

#### off

The switch will use the physical MAC address for all packets except VRRP advertisements.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use this command to change which MAC address the switch will use as the source MAC when sending packets from a VRRP instance.
- This command has no affect on VRRP advertisements, the VRRP virtual MAC will always be used.

### Examples

```
-> ipv6 virtual-source-mac on
-> ipv6 virtual-source-mac off
```

### Release History

Release 7.2.1; command was introduced.
**Related Commands**

`show ipv6 route-pref` Displays the configured route preference of a router.

**MIB Objects**

N/A
ipv6 echo

Configures the switch to reply or ignore echo requests in response to an echo request sent to a multicast or anycast IPv6 address. Use no option to ignore reply to anycast or multicast echo requests.

ipv6 echo {anycast | multicast}
no ipv6 echo {anycast | multicast}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>anycast</td>
<td>Ignore (when no option is used) or reply to anycast echo requests.</td>
</tr>
<tr>
<td>multicast</td>
<td>Ignore (when no option is used) or reply to multicast echo requests.</td>
</tr>
</tbody>
</table>

Defaults

By default, the switch will reply to multicast or anycast echo requests.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The switch will not ignore echo requests that it originates that are destined to one of its own anycast or multicast addresses.

Examples

- -> ipv6 echo multicast
- -> no ipv6 echo anycast

Release History

Release 8.4.1; command introduced.

Related Commands

- show ipv6 information Displays IPv6 information.

MIB Objects

- alaIPv6IgnoreAnycastEchos
- alaIPv6IgnoreMcastEchos
ipv6 icmp rate-limit

Configures the rate-limiting of ICMPv6 error messages.

ipv6 icmp rate-limit [interval number] [burst number]

no ipv6 icmp rate-limit

**Syntax Definitions**

interval number The minimum interval between the ICMPv6 error messages. Valid range is 0 to 10000 in milliseconds.

burst number The maximum number of ICMPv6 error messages that may be sent in a single burst regardless of the interval. Valid range is 1 to 50.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval number</td>
<td>10ms</td>
</tr>
<tr>
<td>burst number</td>
<td>10</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>X</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use no option to disable the ICMPv6 error message rate limiting.

**Examples**

- -> ipv6 icmp rate-limit interval 100
- -> ipv6 icmp rate-limit burst 20
- -> no ipv6 icmp rate-limit

**Release History**

Release 8.4.1; command introduced.
Related Commands

show ipv6 information  Displays IPv6 information.

MIB Objects

alaIPv6IcmpRateLimitInterval
alaIPv6IcmpRateLimitBurst
**ping6**

Tests whether an IPv6 destination can be reached from the local switch. This command sends an ICMPv6 echo request to a destination and then waits for a reply. To ping a destination, enter the `ping6` command and enter either the destination’s IPv6 address or hostname. The switch will ping the destination using the default frame count, packet size, and interval (6 frames, 64 bytes, and 1 second respectively). You can also customize any or all of these parameters as described below.

`ping6 {ipv6_address | hostname} [if_name] [count count] [size data_size] [interval seconds]`

### Syntax Definitions

- **ipv6_address**
  - The IP address of the system to ping.

- **hostname**
  - DNS name of the system to ping.

- **if_name**
  - If the target is a link-local address, the name of the interface used to reach it.

- **count**
  - Number of packets to be transmitted.

- **size**
  - Size of the data portion of the packet sent for this ping, in bytes.

- **seconds**
  - Interval, in seconds, at which ping packets are transmitted.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>6</td>
</tr>
<tr>
<td>size</td>
<td>8</td>
</tr>
<tr>
<td>interval seconds</td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If you change the default values, they will only apply to the current ping. The next time you use the `ping` command, the default values will be used unless you again enter different values.

- When the next hop address is a local link address, the name of the interface used to reach the destination must be specified.

### Examples

```
-> ping6 2001:db8:302::44
```
-> ping6 fe80::2d0:95ff:fe6a:f458 vlanif-23

**Release History**
Release 7.1.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute6</td>
<td>Finds the path taken by an IPv6 packet from the local switch to a specified destination.</td>
</tr>
</tbody>
</table>

**MIB Objects**

N/A
**traceroute6**

Finds the path taken by an IPv6 packet from the local switch to a specified destination. This command displays the individual hops to the destination as well as some timing information.

```
traceroute6 {ipv6_address | hostname} [if_name] [max-hop hop_count] [dest-port port_number] [probe-count probe] [size size] [host-names {yes | no}]
```

**Syntax Definitions**

- **ipv6_address**: Destination IPv6 address. IPv6 address of the host whose route you want to trace.
- **hostname**: DNS name of the host whose route you want to trace.
- **if_name**: If the target is a link-local address, the name of the interface used to reach it.
- **hop_count**: Maximum hop count for the trace.
- **port_number**: Specific UDP port destination. By default, the destination port is chosen by traceroute6.
- **probe**: Number of probes to be sent to a single hop.
- **size**: The initial size for the probe packet. During the trace the packet size will be adjusted downward as path MTU information is received. The default and maximum value is 24,000 bytes with a minimum of 1,280 bytes.
- **host-names {yes | no}**: Specify whether each hop must be shown as an IPv6 address or the host name corresponding to the address.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hop_count</td>
<td>32</td>
</tr>
<tr>
<td>probe</td>
<td>3</td>
</tr>
<tr>
<td>host-names</td>
<td>no</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C6/T48C6/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes  Yes
**Usage Guidelines**

- When using this command, you must enter the name of the destination as part of the command line (either the IPv6 address or hostname).
- Use the optional **max-hop** parameter to set a maximum hop count to the destination. If the trace reaches this maximum hop count without reaching the destination, the trace stops.

**Examples**

```
-> traceroute6 41EA:103::65C3
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ping6**
  Tests whether an IPv6 destination can be reached from the local switch.

**MIB Objects**

| N/A |
modify boot parameters

This command is used to configure IPv6 EMP interface.

modify boot parameters

Syntax Definitions

N/A

Defaults

By default, the EMP interface will have the following configuration.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>baudrate</td>
<td>9600</td>
</tr>
<tr>
<td>parity</td>
<td>none</td>
</tr>
<tr>
<td>wordsize</td>
<td>8</td>
</tr>
<tr>
<td>stopbits</td>
<td>1</td>
</tr>
<tr>
<td>mode</td>
<td>modemControlOff</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- You must be on the system console to modify the system boot parameters. Enter `modify boot parameters` command. This enters the `boot` mode. IPv6 EMP interface parameters like the unique IP address and mask, baudrate, priority, and so on can be configured after entering the boot mode.
- Only one IPv6 EMP interface is allowed per physical EMP port in the default VRF.
- It is required to configure an unique IPv6 Address that does not conflict with any other IPv6 interface configured in the system.
- It is required to reload the switch for the modified interface configuration to come into effect.

Examples

```
-> modify boot parameters
Please wait...
Type '?' for help, 'exit' to exit the boot param parser.
Boot > ?
boot empipaddr  <ip address>
boot empmasklength <number of bits in mask>
```
IPv6 Commands

modify boot parameters

IPv6 Commands modify boot parameters

`boot serialbaudrate` <1200, 2400, 4800, 9600, 19200, 38400, 57600, 76800, 115200>
`boot serialparity` <none, even, odd>
`boot serialwordsize` <7, 8>
`boot serialstopbits` <1, 2>
`boot serialmode` <modemControlOn, modemControlOff>
`boot empipv6addr` <ipv6 address>
`boot empipv6masklength` <number of bits in mask>

'`show'` - Display the edit buffer
'`commit boot'` - Commit the changes to non volatile memory for future boots
'`commit system'` - Commit the changes to running system ONLY
Note: EMP changes will only take effect on a future boot
'`exit'` - Exit (quit)

`show` command displays the existing configuration of EMP interface.

Boot > show
EMP IP Address : 10.200.105.21/24
Serial (console) baud : 9600
Serial (console) parity : none
Serial (console) wordsize : 8
Serial (console) stopbits : 1
Serial (console) mode : modemControlOff
EMP IPV6 Address : /

To Configure IPv6 EMP interface, configure the IP address and mask:

Boot > boot empipv6masklength 64
Boot > show
EMP IP Address : 10.200.105.21/24
Serial (console) baud : 9600
Serial (console) parity : none
Serial (console) wordsize : 8
Serial (console) stopbits : 1
Serial (console) mode : modemControlOff
EMP IPV6 Address : /64

Boot > boot empipv6addr 2001::205
Boot > show
EMP IP Address : 10.200.105.21/24
Serial (console) baud : 9600
Serial (console) parity : none
Serial (console) wordsize : 8
Serial (console) stopbits : 1
Serial (console) mode : modemControlOff
EMP IPV6 Address : 2001::205/64
Boot >

**Release History**

Release 8.4.1; command introduced.
**Related Commands**

- `show ipv6 interface`: Displays IPv6 interface configuration.
- `show ipv6 emp-interface`: Displays the IPv6 EMP interface configuration.
- `show ipv6 emp-routes`: Displays the IPv6 routes targeted to EMP port/IPv6 EMP interface configuration.

**MIB Objects**

N/A
**show ipv6 icmp statistics**

Displays IPv6 ICMP statistics.

`show ipv6 icmp statistics [if_name]`

**Syntax Definitions**

*if_name*  
Display statistics only for this interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the ICMP table to monitor and troubleshoot the switch.

**Examples**

```plaintext
-> show ipv6 icmp statistics
Message                      Current | Previous | Change
----------------------------+----------+----------+----------
Received Total                857      | 0        | 857      
    Errors                    0        | 0        | 0        
    Destination Unreachable  0        | 0        | 0        
    Packet Too Big            0        | 0        | 0        
    Time Exceeded             0        | 0        | 0        
    Parameter Problems        0        | 0        | 0        
    Echo Requests             0        | 0        | 0        
    Echo Replies               0        | 0        | 0        
    Group Membership Queries  0        | 0        | 0        
    Group Membership Responses 0       | 0        | 0        
    Group Membership Reductions 0       | 0        | 0        
    Router Solicitations      9        | 0        | 9        
    Router Advertisements     847      | 0        | 847      
    Neighbor Solicitations    1        | 0        | 1        
    Neighbor Advertisements   0        | 0        | 0        
    Redirects                 0        | 0        | 0        
    Administratively Prohibited 0       | 0        | 0        
Sent Total                   18       | 0        | 18       
    Errors                    0        | 0        | 0        
    Destination Unreachable  0        | 0        | 0        
    Packet Too Big            0        | 0        | 0        
```
IPv6 Commands

Time Exceeded 0 0 0
Parameter Problems 0 0 0
Echo Requests 0 0 0
Echo Replies 0 0 0
Group Membership Queries 0 0 0
Group Membership Responses 11 0 11
Group Membership Reductions 0 0 0
Router Solicitations 3 0 3
Router Advertisements 0 0 0
Neighbor Solicitations 4 0 4
Neighbor Advertisements 0 0 0
Redirects 0 0 0
Administratively Prohibited 0 0 0

output definitions

<table>
<thead>
<tr>
<th>Total</th>
<th>Total number of ICMPv6 messages the switch received or attempted to send.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Errors</td>
<td>Number of ICMPv6 messages the switch sent or received but was unable to process because of ICMPv6-specific errors (bad checksums, bad length, etc.).</td>
</tr>
<tr>
<td>Destination Unreachable</td>
<td>Number of Destination Unreachable messages that were sent or received by the switch.</td>
</tr>
<tr>
<td>Packet Too Big</td>
<td>Number of Packet Too Big messages sent or received by the switch.</td>
</tr>
<tr>
<td>Administratively Prohibited</td>
<td>Number of Destination Unreachable/Communication Administratively Prohibited messages sent or received by the switch.</td>
</tr>
<tr>
<td>Time Exceeded</td>
<td>Number of Time Exceeded messages sent or received by the switch.</td>
</tr>
<tr>
<td>Parameter Problems</td>
<td>Number of Parameter Problem messages sent or received by the switch.</td>
</tr>
<tr>
<td>Echo Requests</td>
<td>Number of Echo Request messages sent or received by the switch.</td>
</tr>
<tr>
<td>Echo Replies</td>
<td>Number of Echo Reply messages sent or received by the switch.</td>
</tr>
<tr>
<td>Group Membership Queries</td>
<td>Number of Group Membership Queries sent or received by the switch.</td>
</tr>
<tr>
<td>Group Membership Responses</td>
<td>Number of Group Membership Responses sent or received by the switch.</td>
</tr>
<tr>
<td>Group Membership Reductions</td>
<td>Number of Group Membership Reductions sent or received by the switch.</td>
</tr>
<tr>
<td>Router Solicitations</td>
<td>Number of Router Solicitations sent or received by the switch.</td>
</tr>
<tr>
<td>Router Advertisements</td>
<td>Number of Router Advertisements sent or received by the switch.</td>
</tr>
<tr>
<td>Neighbor Solicitations</td>
<td>Number of Neighbor Solicitations sent or received by the switch.</td>
</tr>
<tr>
<td>Neighbor Advertisements</td>
<td>Number of Neighbor Advertisements sent or received by the switch.</td>
</tr>
<tr>
<td>Redirects</td>
<td>Number of Redirect messages sent or received by the switch.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 traffic* Displays IPv6 traffic statistics.

**MIB Objects**

ipv6IfIcmpTable
  - ipv6IfIcmpInMsgs
  - ipv6IfIcmpInErrors
  - ipv6IfIcmpInDestUnreachs
  - ipv6IfIcmpInAdminProhibs
  - ipv6IfIcmpInTimeExcds
  - ipv6IfIcmpInParmProblems
  - ipv6IfIcmpInPktTooBigs
  - ipv6IfIcmpInEchos
  - ipv6IfIcmpInEchoReplies
  - ipv6IfIcmpInRouterSolicits
  - ipv6IfIcmpInRouterAdvertisements
  - ipv6IfIcmpInNeighborSolicits
  - ipv6IfIcmpInRedirects
  - ipv6IfIcmpInGroupMembQueries
  - ipv6IfIcmpInGroupMembResponses
  - ipv6IfIcmpInGroupMembRevisions
  - ipv6IfIcmpOutMsgs
  - ipv6IfIcmpOutErrors
  - ipv6IfIcmpOutDestUnreachs
  - ipv6IfIcmpOutAdminProhibs
  - ipv6IfIcmpOutTimeExcds
  - ipv6IfIcmpOutParmProblems
  - ipv6IfIcmpOutPktTooBigs
  - ipv6IfIcmpOutEchos
  - ipv6IfIcmpOutEchoReplies
  - ipv6IfIcmpOutRouterSolicits
  - ipv6IfIcmpOutRouterAdvertisements
  - ipv6IfIcmpOutNeighborSolicits
  - ipv6IfIcmpOutNeighborAdvertisements
  - ipv6IfIcmpOutRedirects
  - ipv6IfIcmpOutGroupMembQueries
  - ipv6IfIcmpOutGroupMembResponses
  - ipv6IfIcmpOutGroupMembReductions
show ipv6 interface

Displays the configuration and status of IPv6 interfaces.

show ipv6 interface [if_name | loopback]

Syntax Definitions

*if_name*  
Interface name. Limits the display to a specific interface.

*loopback*  
Limits display to loopback interfaces.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If an interface name is not specified, all IPv6 interfaces are displayed.
- Specify an interface name (e.g., VLAN 12) to obtain a more detailed information about a specific interface.

Examples

```
-> show ipv6 interface
Name                      IPv6 Address/Prefix Length     Status     Device
------------------------------------------------------------------------------------------------------
smbif-5                    fe80::2d0:95ff:fe12:f470/64      Active     VLAN 955
                            212:95:5::35/64
                            212:95:5::/64
if-200                     fe80:::eae7:32ff:fe4:6321/64      Inactive   VLAN 200
                            2002:d423:2323::35/64
                            2002:d423:2323::/64
v6if-tunnel-137            fe80::2d0:95ff:fe12:f470/64      Disabled   Tunnel 2
                            137:35:35::35/64
                            137:35:35::/64
loopback                   ::1/128                                 Active     Loopback
EMF-CMMA-CHAS1             2001::205/64                     Active     EMP
                            fe80:::eae7:32ff:fe4:6321/64
vpnl                       fe80::2b0:d0ff:fe86:880e/64      Active     Service 1
                            2001:db8:1000::2b0:d0ff:fe86:880e/64
rp-10                      fe80::2b0:d0ff:fe86:880e/64      Active     VLAN 10 1/1/2
rp_11                      fe80::2b0:d0ff:fe86:880e/64      Active     VLAN 11 agg 7
```
-> show ipv6 interface if-200

if-200
IPv6 interface index = 200(0x000000c8)
Administrative status = Enabled
Operational status = Inactive
Hardware address = e8:e7:32:a4:63:21
Device = VLAN 200
Link-local address(es):
  fe80::eae7:32ff:fea4:6321/64
Global unicast address(es):
Anycast address(es):
VRRP address(es):
Joined group addresses:
  ff01::1
  ff02::1
  ff02::2
Maximum Transfer Unit (MTU) = 1500
Neighbor reachable time (sec) = 346
Base reachable time (sec) = 360
Retransmit timer (ms) = 1000
Retransmit backoff = 1
Retransmit max = 3
DAD transmits = 1
Send Router Advertisements = Yes
Maximum RA interval (sec) = 600
Minimum RA interval (sec) = 198
RA managed config flag = False
RA other config flag = False
RA reachable time (ms) = 0
RA retransmit timer (ms) = 0
RA default lifetime (sec) = 1800
RA hop limit = 64
RA send MTU option = No
RA send RDNSS option = No
RA send DNSSL option = No
RA clock skew (sec) = 600
RA router preference = Medium
RA filtering = Disabled
Neighbor cache limit = None
Local Proxy ND = Disabled

-> show ipv6 interface EMP-CMMA-CHAS1

EMP-CMMA-CHAS1
IPv6 interface index = 67108865(0x04000001)
Administrative status = Enabled
Operational status = Active
Hardware address = e8:e7:32:a4:a1:a8
Device                        = EMP
Link-local address(es):
    fe80::eae7:32ff:fea4:a1a8/64
Global unicast address(es):
    2001::205/64
Anycast address(es):
VRRP address(es):
Joined group addresses:
    ff01::1
    ff01::2
    ff02::1
    ff02::1:ff00:205
    ff02::202
    ff02::1:ffa4:a1a8
    ff02::2
    ff02::1:ff00:0
    ff05::2
Maximum Transfer Unit (MTU)   = 1500
Neighbor reachable time (sec) = 420
Base reachable time (sec)     = 360
Retransmit timer (ms)         = 1000
Retransmit backoff            = 1
Retransmit max                = 3
DAD transmits                 = 1
Send Router Advertisements    = No
Maximum RA interval (sec)     = 600
Minimum RA interval (sec)     = 198
RA managed config flag        = False
RA other config flag          = False
RA reachable time (ms)        = 0
RA retransmit timer (ms)      = 0
RA default lifetime (sec)     = 1800
RA hop limit                  = 64
RA send MTU option            = No
RA send RDNSS option          = No
RA send DNSSSL option         = No
RA clock skew (sec)           = 600
RA router preference          = Medium
Neighbor cache limit          = None

-> show ipv6 interface vpn1
vpn1
   IPv6 interface index          = 100663297(0x06000001)
   Administrative status        = Enabled
   Operational status           = Inactive
   Hardware address             = e8:e7:32:1e:4c:88
   Device                       = Service 1
Link-local address(es):
    fe80::eae7:32ff:fe1e:4c88/64
Global unicast address(es):
    2001:db8:1000::2b0:d0ff:fe86:880e/64
Anycast address(es):
VRRP address(es):
Joined group addresses:
    ff01::1
    ff02::1
    ff02::2
Maximum Transfer Unit (MTU)   = 1500
Neighbor reachable time (sec) = 284
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base reachable time (sec)</td>
<td>360</td>
</tr>
<tr>
<td>Retransmit timer (ms)</td>
<td>1000</td>
</tr>
<tr>
<td>Retransmit backoff</td>
<td>1</td>
</tr>
<tr>
<td>Retransmit max</td>
<td>3</td>
</tr>
<tr>
<td>DAD transmits</td>
<td>1</td>
</tr>
<tr>
<td>Send Router Advertisements</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum RA interval (sec)</td>
<td>600</td>
</tr>
<tr>
<td>Minimum RA interval (sec)</td>
<td>198</td>
</tr>
<tr>
<td>RA managed config flag</td>
<td>False</td>
</tr>
<tr>
<td>RA other config flag</td>
<td>False</td>
</tr>
<tr>
<td>RA reachable time (ms)</td>
<td>0</td>
</tr>
<tr>
<td>RA retransmit timer (ms)</td>
<td>0</td>
</tr>
<tr>
<td>RA default lifetime (sec)</td>
<td>1800</td>
</tr>
<tr>
<td>RA hop limit</td>
<td>64</td>
</tr>
<tr>
<td>RA send MTU option</td>
<td>No</td>
</tr>
<tr>
<td>RA send RDNSS option</td>
<td>No</td>
</tr>
<tr>
<td>RA send DNSSL option</td>
<td>Yes</td>
</tr>
<tr>
<td>RA clock skew (sec)</td>
<td>600</td>
</tr>
<tr>
<td>RA router preference</td>
<td>Medium</td>
</tr>
<tr>
<td>RA filtering</td>
<td>Disabled</td>
</tr>
<tr>
<td>Neighbor cache limit</td>
<td>None</td>
</tr>
<tr>
<td>Local Proxy ND</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

```
-> show ipv6 interface rp_10
rp_10
IPv6 interface index       = 100663297(0x06000001)
Administrative status      = Enabled
Operational status         = Inactive
Hardware address           = e8:e7:32:1e:4c:88
Device                     = VLAN 10 1/1/1
tagged
Routed Port                = 1/1/1
Link-local address(es):
  fe80::eae7:32ff:fe1e:4c88/64
Global unicast address(es):
  2001:db8:1000::2b0:d0ff:fe86:880e/64
Anycast address(es):
VRRP address(es):
Joined group addresses:
  ff01::1
  ff02::1
  ff02::2
Maximum Transfer Unit (MTU) = 1500
Neighbor reachable time (sec) = 284
Base reachable time (sec)    = 360
Retransmit timer (ms)        = 1000
Retransmit backoff           = 1
Retransmit max               = 3
DAD transmits                = 1
Send Router Advertisements  = Yes
Maximum RA interval (sec)    = 600
Minimum RA interval (sec)    = 198
RA managed config flag       = False
RA other config flag         = False
RA reachable time (ms)       = 0
RA retransmit timer (ms)     = 0
RA default lifetime (sec)    = 1800
RA hop limit                 = 64
RA send MTU option           = No
RA send RDNSS option         = No
```
<table>
<thead>
<tr>
<th>Output Definitions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 interface index</td>
<td>IPv6IfIndex value that must be used in SNMP requests pertaining to this interface.</td>
</tr>
<tr>
<td>Administrative status</td>
<td>Administrative status of this interface (Enabled/Disabled).</td>
</tr>
<tr>
<td>Operational status</td>
<td>Indicates whether the physical interface is connected to a device (Active/Inactive).</td>
</tr>
<tr>
<td>Hardware address</td>
<td>The hardware address.</td>
</tr>
<tr>
<td>Device</td>
<td>The device on which the interface is configured (for example, VLAN 955). This field will also display the port or link aggregate assignment for IPv6 routed-port interfaces (for example, “VLAN 10 1/1/2”)</td>
</tr>
<tr>
<td>Routed Port</td>
<td>This field appears only for routed port interfaces and displays the tag status (tagged or untagged) of the port or link aggregate that is associated with the routed port interface.</td>
</tr>
<tr>
<td>Link-local address</td>
<td>Link-local address assigned to the interface.</td>
</tr>
<tr>
<td>Global unicast address(es)</td>
<td>Global unicast address(es) assigned to the interface.</td>
</tr>
<tr>
<td>Anycast address(es)</td>
<td>The anycast address(es) assigned to this interface.</td>
</tr>
<tr>
<td>VRRP address(es)</td>
<td>Addresses assigned to the interface because a VRRP virtual router is active. If (accept) is present, the switch will accept packets destined to the address. If not present, any such packets will be discarded.</td>
</tr>
<tr>
<td>Joined group address(es)</td>
<td>Addresses of the multicast groups that this interface has joined.</td>
</tr>
<tr>
<td>Maximum Transfer Unit</td>
<td>Interface MTU value.</td>
</tr>
<tr>
<td>Neighbor reachable time (sec)</td>
<td>The amount of time that a neighbor reached through this interface will remain in the reachable state.</td>
</tr>
<tr>
<td>Base reachable time (sec)</td>
<td>The base reachable time used to calculate the current neighbor reachable time.</td>
</tr>
<tr>
<td>Retransmit timer (ms)</td>
<td>The interval at which neighbour solicitations will be retransmitted during the neighbor discovery process.</td>
</tr>
<tr>
<td>Retransmit backoff</td>
<td>The NUD exponential backoff base value.</td>
</tr>
<tr>
<td>Retransmit max</td>
<td>The maximum number of neighbor solicitations to be sent during ND/NUD.</td>
</tr>
<tr>
<td>DAD transmits</td>
<td>The number of neighbour solicitations that will be sent as part of the Duplicate Address Detection process.</td>
</tr>
<tr>
<td>Send Router Advertisements</td>
<td>Indicates if the router sends periodic router advertisements and responds to router solicitations on the interface.</td>
</tr>
<tr>
<td>Maximum RA interval (sec)</td>
<td>Maximum time between the transmission of unsolicited router advertisements over the interface.</td>
</tr>
<tr>
<td>Minimum RA interval (sec)</td>
<td>Minimum time between the transmission of unsolicited router advertisements over the interface (0.33 * Maximum RA Interval).</td>
</tr>
<tr>
<td>RA managed config flag</td>
<td>True/False value in the managed address configuration flag field in router advertisements.</td>
</tr>
</tbody>
</table>
### Output Definitions (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA other config flag</td>
<td>The True/False value in the other stateful configuration flag field in router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA reachable time (ms)</td>
<td>Value placed in the reachable time field in the router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA retransmit timer (ms)</td>
<td>Value placed in the retransmit timer field in router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA default lifetime (sec)</td>
<td>The value placed in the router lifetime field in the router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA hop limit</td>
<td>The value placed in the current hop limit field in the router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA Send MTU option</td>
<td>Specifies whether the MTU option is included in the router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA Send RDNSS option</td>
<td>Specifies whether the RDNSS option is included in the router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA Send DNSSL option</td>
<td>Specifies whether the DNSSL option is included in the router advertisements sent over this interface.</td>
</tr>
<tr>
<td>RA clock skew (sec)</td>
<td>The clock skew allowed for router advertisements on this interface.</td>
</tr>
<tr>
<td>RA filtering</td>
<td>Specifies if RA filtering is enabled or disabled on the interface.</td>
</tr>
<tr>
<td>Neighbor cache limit</td>
<td>The interface’s neighbor cache limit. “none” if value not set.</td>
</tr>
<tr>
<td>RA router preference</td>
<td>Specifies the router preference - medium, high, low.</td>
</tr>
<tr>
<td>Local Proxy ND</td>
<td>Specifies if Local Proxy Neighbor Discovery is enabled or disabled on the interface.</td>
</tr>
</tbody>
</table>

### Release History

- **Release 7.1.1**: command was introduced.
- **Release 8.4.1**: EMP interface information added.
- **Release 8.5R4**: service-based interface information added.
- **Release 8.6R2**: “Device” and “Routed Port” fields added.
- **Release 8.7R1**: “RA send DNSSL option” and “RA send RDNSS option” fields added.

### Related Commands

- **ipv6 address**: Configures an IPv6 address for an IPv6 interface.
- **ipv6 interface**: Configures an IPv6 interface.
- **ipv6 interface rtr-port**: Configures an IPv6 routed-port interface.
- **modify boot parameters**: Configures the IPv6 EMP interface.
**MIB Objects**

ipv6IfTable
  ipv6IfIndex
  ipv6IfAdminStatus
  ipv6IfOperStatus
  ipv6IfPhysicalAddress

ipv6AddrTable
  ipv6AddrAddress
  ipv6AddrPfxLength

alaIPv6InterfaceAddressTable
  alaIPv6InterfaceAddress
  alaIPv6InterfaceAddressPrefixLength
  alaIPv6InterfaceAddressAnycastFlag

alaIPv6InterfaceTable
  alaIPv6InterfaceName
  alaIPv6InterfaceDescription
  alaIPv6InterfaceAddressVRRPFlag
  alaIPv6MulticastGroupAddress
  alaIPv6InterfaceMtu
  alaIPv6InterfaceReachableTime
  alaIPv6InterfaceBaseReachableTime
  alaIPv6InterfaceRetransTimer
  alaIPv6InterfaceRetransBackoff
  alaIPv6InterfaceRetransMax
  alaIPv6InterfaceDADTransmits
  alaIPv6InterfaceAddressDADStatus
  alaIPv6InterfaceSendRouterAdvertisements
  alaIPv6InterfaceMaxRtrAdvInterval
  alaIPv6InterfaceMinRtrAdvInterval
  alaIPv6InterfaceAdvManagedFlag
  alaIPv6InterfaceAdvOtherConfigFlag
  alaIPv6InterfaceAdvReachableTime
  alaIPv6InterfaceAdvRetransTimer
  alaIPv6InterfaceAdvDefaultLifetime
  alaIPv6InterfaceAdvHopLimit
  alaIPv6InterfaceAdvSendMtu
  alaIPv6InterfaceAdvSendDNSSL
  alaIPv6InterfaceAdvSendRDNSS
  alaIPv6InterfaceClockSkew
  alaIPv6InterfaceRAFilter
  alaIPv6InterfaceNeighborLimit
  alaIPv6InterfaceLPND
**show ipv6 emp-interface**

Displays the IPv6 EMP interface configuration.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ipv6 emp-interface
Name             IPv6 Address/Prefix Length     Status  Device
----------------+----------------------------------------+---------+--------
EMP-CMMA-CHAS1   2001::205/64               Active  EMP
                 fe80::eae7:32ff:fea4:a1a8/64          
```

**output definitions**

<table>
<thead>
<tr>
<th>Name</th>
<th>Interface name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address/Prefix Length</td>
<td>IPv6 address and prefix length assigned to the interface. If an interface has more than one IPv6 address assigned to it, each address is shown on a separate line.</td>
</tr>
<tr>
<td>Status</td>
<td>Interface status (Active/Inactive/Disabled).</td>
</tr>
<tr>
<td>Device</td>
<td>The device on which the interface is configured.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.4.1; command introduced.
Related Commands

modify boot parameters

This command is used to configure IPv6 EMP interface.

MIB Objects

N/A
show ipv6 emp-routes

Displays the IPv6 routes targeted to EMP port/IPv6 EMP interface configuration.

show ipv6 emp-routes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>69009900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 emp-routes
Legend: Flags: U=Up, G=Gateway, H=Host, S=Static, C=Cloneable, B=Discard, E=ECMP

Total 2 routes

<table>
<thead>
<tr>
<th>Destination/Prefix</th>
<th>Gateway Address</th>
<th>Interface</th>
<th>Age</th>
<th>Protocol</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::/64</td>
<td>::</td>
<td>EMP-CMMA-CHAS1</td>
<td>1d</td>
<td>LOCAL</td>
<td>UC</td>
</tr>
<tr>
<td>4001::/64</td>
<td>2001::9</td>
<td>EMP-CMMA-CHAS1</td>
<td>1d</td>
<td>STATIC</td>
<td>UGS</td>
</tr>
</tbody>
</table>

output definitions

- **Destination/Prefix**: The destination IPv6 address of the IPv6 EMP route.
- **Gateway Address**: The next hop IPv6 address to reach the destination.
- **Interface**: The interface through which the destination IPv6 address is reachable.
- **Age**: Time since this route was last updated or otherwise determined to be correct.
**output definitions**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>The routing mechanism through which this route was learned. For EMP routes, this can be only local or static. Routing protocol are not supported on EMP interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Route flags that describes the route details.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.4.1; command introduced.

**Related Commands**

- **ipv6 static-route** Configures an IPv6 static route.

**MIB Objects**

- ipv6RouteDest
- ipv6RoutePfxLength
- ipv6RouteNextHop
- alaIPv6InterfaceName
- ipv6RouteAge
- ipv6RouteProtocol
show ipv6 pmtu table

Displays the IPv6 Path MTU Table.

show ipv6 pmtu table

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 pmtu table

1-PMTU Entry
PMTU entry minimum lifetime = 10m

<table>
<thead>
<tr>
<th>Destination Address</th>
<th>MTU</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::02d0:c0ff:fe86:1207</td>
<td>1280</td>
<td>1h 0m</td>
</tr>
</tbody>
</table>

output definitions

- Destination Address: IPv6 address of the path's destination.
- MTU: Path's MTU.
- Expires: Minimum remaining lifetime for the entry.

Release History

Release 7.1.1; command was introduced.
**Related Commands**

`ipv6 pmtu-lifetime`  
Configures the minimum lifetime for entries in the path MTU Table.

**MIB Objects**

alaIPv6ConfigTable
alaIPv6PMTUDest
alaIPv6PMTUexpire
**show ipv6 ra-filter**

Displays the RA filter configuration for an IPv6 interface.

`show ipv6 ra-filter [if-name]`

### Syntax Definitions

`if_name` IPV6 interface name.

### Defaults

By default, the RA filter configuration is displayed for all IPv6 VLAN interfaces.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `if-name` parameter to display information for a specific IPv6 interface.

### Examples

```
-> show ipv6 ra-filter
Interface                        Status   Trusted Ports
--------------------------------+--------+----------------------------------------
vlan-23                          Enabled  1/1/22, agg 7
vlan-24                          Enabled  none
```

**output definitions**

- **Interface**: Displays the IPv6 VLAN interface on which RA filtering is configured.
- **Status**: Displays the status of RA filtering on the interface. The interfaces on which the RA filtering is disabled are displayed only if one or more trusted ports are configured for the interface.
- **Trusted Ports**: Displays the RA filtering trusted sources for the interface. A '+' will appear at the end of the list to indicate that there are more trusted sources configured which cannot be displayed in a single line. To view the full list of configured trusted sources, specify the interface name in the `show` command as recommended.

```
-> show ipv6 ra-filter vlan-23
RA Filtering: Enabled
Trusted ports: 1/1/22
 agg 7
```
output definitions

<table>
<thead>
<tr>
<th>RA Filtering</th>
<th>Indicates if RA filtering is enabled or disabled on the IPv6 VLAN interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted ports</td>
<td>Shows the RA filtering trusted ports (chassis/slot/port) or link aggregates (linkagg ID) for the interface. Displays none if there are no trusted ports.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command introduced.
Release 8.5R2; OmniSwitch 6560 support for IPv6 RA Filtering added.

Related Commands

ipv6 ra-filter Enables or disables the status of RA filtering on IPv6 VLAN interfaces. When enabled, any RAs received on associated ports and link aggregates are discarded.

ipv6 ra-filter trusted Configures the RA filtering trust status for ports and link aggregates associated with the IPv6 VLAN interface. When a port or link aggregate is trusted, it can accept RAs received when the RA filtering status is enabled.

MIB Objects

IPv6IfIndex

alaIPv6RAFilterTrustedChassis
alaIPv6RAFilterTrustedSlot
alaIPv6RAFilterTrustedPort
**show ipv6 neighbors**

Displays IPv6 Neighbor Table.

```
show ipv6 neighbors [ipv6_prefix/prefix_length | if_name | hw hardware_address | static]
```

### Syntax Definitions

**ipv6_prefix/prefix_length**
IPv6 prefix. Restricts the display to those neighbors starting with the specified prefix.

**if_name**
Interface name. Restricts the display to those neighbors reached through the specified interface.

**hardware_address**
MAC address. Restricts the display to the specified MAC address.

**static**
Restricts display to statically configured neighbors.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you do not specify an option (e.g., if_name), all IPv6 neighbors are displayed.

### Examples

```
-> show ipv6 neighbors
Total 4 neighbors

IPv6 Address           Hardware Address  Reachability Lifetime Port  Interface
-----------------------+-----------------+------------+--------+--------------+---------
2001:db8:9::88         00:d0:95:01:0a:ec Confirmed       5m 5s 1/3/7          vlan_7
fe80::2d0:95ff:fe01:aec 00:d0:95:01:0a:ec Confirmed       5m 6s 1/3/7          vlan_7
2001:db8:1000::100     00:d0:95:a8:08:11 Confirmed       2m 20s sap:1/3/9:1000 vpn1
2001:db8:1000::101     00:d0:95:c3:19:aa Confirmed       1m 23s sdp:32768:1000 vpn1
```

### output definitions

- **IPv6 Address**: The neighbor’s IPv6 address.
- **Hardware Address**: The MAC address corresponding to the IPv6 address.
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reachability</td>
<td>The neighbor’s reachability:</td>
</tr>
<tr>
<td></td>
<td>• Incomplete</td>
</tr>
<tr>
<td></td>
<td>• Confirmed</td>
</tr>
<tr>
<td></td>
<td>• Unconfirmed</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The time the entry will remain in its current state.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used to reach the neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>The neighbor’s interface name (e.g., vlan_1).</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; neighbor information for service-based interfaces added.

Related Commands

ipv6 neighbor Configures a static entry in the IPv6 Neighbor Table.

MIB Objects

ipv6IfIndex
alaIPv6NeighborTable
    alaIPv6NeighborNetAddress
    alaIPv6NeighborPhysAddress
    alaIPv6NeighborReachability
    alaIPv6NeighborLifetime
    alaIPv6NeighborType
    alaIPv6NeighborPortIfIndex
    alaIPv6NeighborPortType
    alaIPv6NeighborPortSubId
clear ipv6 neighbors

Removes all entries, except static entries, from IPv6 Neighbor Table.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command only clears dynamic entries. If static entries have been added to the table, they must be removed using the no form of the ipv6 neighbor command.

Examples

-> clear ipv6 neighbors

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 neighbor Configures a static entry in IPv6 Neighbor Table.
show ipv6 neighbors Displays IPv6 Neighbor Table.

MIB Objects

alaIPv6NeighborTable
alaIPv6ClearNeighbors
show ipv6 prefixes

Displays IPv6 prefixes used in router advertisements.

show ipv6 prefixes

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/8</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 prefixes

Legend: Flags: A = Autonomous Address Configuration, L = OnLink

<table>
<thead>
<tr>
<th>Name</th>
<th>IPv6 Address/Prefix Length</th>
<th>Valid Lifetime</th>
<th>Preferred Lifetime</th>
<th>Flags</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 955</td>
<td>212:95:5::/64</td>
<td>2592000</td>
<td>604800</td>
<td>LA</td>
<td>dynamic</td>
</tr>
<tr>
<td>vlan 1002</td>
<td>195:35::/64</td>
<td>2592000</td>
<td>604800</td>
<td>LA</td>
<td>dynamic</td>
</tr>
<tr>
<td>6to4tunnel</td>
<td>2002:d423:2323::/64</td>
<td>2592000</td>
<td>604800</td>
<td>LA</td>
<td>dynamic</td>
</tr>
<tr>
<td>tunnel 2</td>
<td>137:35:35::/64</td>
<td>2592000</td>
<td>604800</td>
<td>LA</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>The interface name. This is usually the VLAN on which the interface is configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address/Prefix Length</td>
<td>The IPv6 prefix and prefix length for a Router Advertisement Prefix Option.</td>
</tr>
<tr>
<td>Valid Lifetime</td>
<td>Length of time, in seconds, that this prefix will remain valid (i.e., time until deprecation). A value of 4,294,967,295 represents infinity.</td>
</tr>
<tr>
<td>Preferred Lifetime</td>
<td>Length of time, in seconds, that this prefix will remain preferred (i.e., time until deprecation). A value of 4,294,967,295 represents infinity.</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Flags</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>Prefix can be used for onlink determination.</td>
</tr>
<tr>
<td>A</td>
<td>Prefix can be used for autonomous address configuration (i.e., can be used to form a local interface address).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Prefix has been configured by management.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Router Advertisements are using interface prefixes.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**ipv6 prefix**

Configures an IPv6 prefix on an interface. Used for configuring prefixes for router advertisements.

**MIB Objects**

- IPv6AddrPrefixTable
  - IPv6AddressPrefixEntry
  - IPv6AddressPrefixLength
  - IPv6AddressPrefixLinkFlag
  - IPv6AddressPrefixAdvvalidLifetime
  - IPv6AddressPrefixAdvPreferredLifetime
- alaIPv6InterfacePrefixTable
  - alaIPv6InterfacePrefix
  - alaIPv6InterfacePrefixLength
  - alaIPv6InterfacePrefixValidLifetime
  - alaIPv6InterfacePrefixPreferredLifetime
  - alaIPv6InterfacePrefixOnLinkFlag
  - alaIPv6InterfacePrefixsource
**show ipv6 routes**

Displays IPv6 Forwarding Table.

```
show ipv6 routes [ipv6_prefix/prefix_length | summary | protocol [bgp | import | isis | local | ospf | rip | static]]
```

**Syntax Definitions**

- `ipv6_prefix/prefix_length`: IPv6 prefix. Restricts the display to those routes starting with the specified prefix.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

`show ipv6 routes` does not include the EMP interface included in the total routes count.

**Examples**

```
-> show ipv6 routes
Legend: Flags: U=Up, G=Gateway, H=Host, S=Static, C=Cloneable, B=Discard, E=ECMP

Total 5 routes

Destination Prefix | Gateway Address | Interface    | Age           | Protocol | Flags
--------------------|-----------------|--------------|---------------|----------|--------
::/0                | 2002:d468:8a89::137 | v6if-6to4-137 | 18h 47m 26s  | Static   | UGS
137:35:35::/64     | fe80::2d0:95ff:fe12:f470 | v6if-tunnel-137 | 18h 51m 55s  | Local    | UC
195:35::/64        | fe80::2d0:95ff:fe12:f470 | v6if-to-eagle  | 18h 51m 55s  | Local    | UC
212:95:5::/64      | fe80::2d0:95ff:fe12:f470 | smbif-5       | 18h 51m 55s  | Local    | UC
55::/64            | ::               | loopback      | 00:00:13      | STATIC   | UBS
```

**output definitions**

- **Destination Prefix**: IPv6 destination address and prefix.
- **Gateway Address**: IPv6 address of the gateway used to reach the destination network. Gateway address ‘::’ indicates an IPv6 blackhole route.
- **Interface**: The device the interface is using (e.g., VLAN 6to4tunnel); or loopback.
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Age of the entry. Entries less than 1 day old are displayed in hh:mm:ss format. Entries more than 1 day old are displayed in dd:hh format.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol by which the route was learned.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 static-route

Configures a static entry in the IPv6 route.

MIB Objects

IPv6RouteTable
   IPv6Routes
   IPv6RoutesPrefix
   IPv6RoutesStatic
alaIPv6StaticRouteTable
   alaIPv6StaticRouteEntry
show ipv6 route-pref

Displays the IPv6 routing preference of the router.

show ipv6 route-pref

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The IPv6 version of BGP is not supported on the OmniSwitch 6560, OmniSwitch 6570M or OmniSwitch 6465.

**Examples**

```
-> show ipv6 route-pref
   Protocol       Route Preference Value
   -------------------------------
    Local              1
    Static             2
    OSPF               110
    ISISL1             115
    ISISL2             118
    RIP                 120
    EBGP               190
    IBGP               200
    Import             210
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

```
ipv6 route-pref
```

Configures the IPv6 route preference of a router.

**MIB Objects**

```
N/A
```
show ipv6 router database

Displays a list of all routes (static and dynamic) that exist in the IPv6 router database. This database serves as a central repository where routes are first processed for redistribution and where duplicate routes are compared to determine the best route to use. If a route does not appear in the IPv6 router database list, then the switch does not know about it. In the case of dynamically learned routes, this could indicate that the route was never received by the switch.

```
show ipv6 router database [protocol type | gateway ipv6_address | dest ipv6_prefix/prefix_length]
```

**Syntax Definitions**

- **type**: Routing protocol type (local, static, OSPF, RIP, BGP, IS-IS, or IMPORT).
- **ipv6_address**: IPv6 address of the next hop used to reach the destination IPv6 address.
- **ipv6_prefix**: IPv6 network that is the destination of this static route.
- **/prefix_length**: The number of bits that are significant in the IPv6 address (mask). (0...128).

**Defaults**

By default, all routes are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The IPv6 forwarding table is derived from IPv6 router database processing performed by the switch and contains only unique routes that the switch currently uses. Use the `show ipv6 routes` command to view the forwarding table.

- If an expected route does not appear in the IPv6 forwarding table, use the `show ipv6 router database` command to see if the switch knows about the route and/or if a duplicate route with a higher precedence was selected instead.

- The switch compares the protocol of duplicate routes to determine which one to use. Regardless of whether or not a route has a higher priority metric value, protocol determines precedence. Local routes are given the highest level of precedence followed by static, OSFP, RIP, then BGP routes. As a result, a route that is known to the switch may not appear in the IP forwarding table if a duplicate route with a higher protocol precedence exists.
- A list of inactive static routes is also included in the **show ipv6 router database** output display. A route becomes inactive if the interface for its gateway goes down. Inactive routes are unable to get to their destination and further investigation is warranted to determine why their gateway is unavailable.

- Routes that appear as inactive are not included in the main IP router database listing. If an inactive route becomes active, however, it is removed from the inactive list and added to the active route list.

**Examples**

```bash
-> show ipv6 router database
Legend: + indicates routes in use
       b indicates BFD-enabled static route

Total IPRM IPv6 routes: 4

<table>
<thead>
<tr>
<th>Destination/Prefix</th>
<th>Gateway Address</th>
<th>Interface</th>
<th>Protocol</th>
<th>Metric</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ 2001::/64</td>
<td>fe80::2efa:a2ff:fe23:24ca</td>
<td>VL-2059</td>
<td>OSPF</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>+ 2001::/64</td>
<td>fe80::de08:56ff:fe10:b41</td>
<td>VL-2060</td>
<td>OSPF</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>+ 2001:0:1::/64</td>
<td>fe80::2efa:a2ff:fe23:24ca</td>
<td>VL-2059</td>
<td>OSPF</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>+ 55::/6</td>
<td>::</td>
<td>loopback</td>
<td>STATIC</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Inactive Static Routes:

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Destination/Prefix</th>
<th>Gateway Address</th>
<th>Metric</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1510</td>
<td>212:95:5::/64</td>
<td>fe80::2d0:95ff:fe6a:f458</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**output definitions**

- **Destination/Prefix**: IPv6 destination address and prefix.
- **Gateway Address**: IPv6 address of the gateway used to reach the destination network. Gateway address '::' indicates an IPv6 blackhole route.
- **Interface**: The device the interface is using (e.g., VLAN 6to4tunnel); or loopback.
- **Protocol**: Protocol by which this IPv6 address was learned: LOCAL, STATIC, OSPF, RIP, BGP).
- **Metric**: RIP metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.
- **VLAN**: The VLAN on which the route was learned, not forwarded. Note that N/A appears in this field for static routes as they are not learned on a VLAN.

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show ipv6 routes**: Displays the IPv6 Forwarding Table.

**MIB Objects**

- **N/A**
show ipv6 tcp connections

Displays the TCP connections over the IPV6 table.

show ipv6 tcp connections

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 tcp connections

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Port</th>
<th>Remote Address</th>
<th>Port</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:0000:0200::23</td>
<td>23</td>
<td>2001:0000:0400::143</td>
<td>1867</td>
<td>established</td>
</tr>
<tr>
<td>2001:0000:0200::23</td>
<td>8734</td>
<td>2001:0000:0200::19</td>
<td>8735</td>
<td>timeWait</td>
</tr>
</tbody>
</table>

output definitions

- **Local Address**: The local IPV6 address for the TCP connection.
- **Port**: The local port number of the TCP connection.
- **Remote Address**: The remote IPV6 address for the TCP connection.
- **Port**: The remote port number of the TCP connection.
- **State**: The state of the TCP connection.

Release History

Release 7.1.1; command was introduced.
**Related Commands**

**show ipv6 tcp listeners**

Displays the TCP connections over the IPV6 listeners (endpoints awaiting a connection request).

**MIB Objects**

alaRipngInterfaceTable
- alaRipngInterfaceStatus
- alaRipngRouteTag
- alaRipngInvalidTimer
- alaRipngGarbageTimer
- alaRipngHolddownTimer
- alaRipngJitter
- alaRipngTriggeredSends
show ipv6 tcp listeners

Displays the TCP connections over the IPv6 listeners (endpoints awaiting a connection request).

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900</td>
</tr>
<tr>
<td>V72/C32</td>
<td>6900</td>
<td>6900</td>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 tcp listeners

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>::0</td>
<td>21</td>
</tr>
<tr>
<td>::0</td>
<td>23</td>
</tr>
<tr>
<td>::0</td>
<td>80</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Local Address</th>
<th>The local IPv6 address for this TCP listener. A value of ::0 indicates that the listener will accept a connection request sent to any of the switch's addresses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The local port number on which the listener is awaiting connection requests.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Related Commands

show ipv6 tcp connections  Displays the TCP connections over the IPV6 table.

MIB Objects

alaRipngInterfaceTable
  alaRipngInterfaceStatus
  alaRipngRouteTag
  laRipngInvalidTimer
  alaRipngGarbageTimer
  alaRipngHolddownTimer
  alaRipngJitter
  alaRipngTriggeredSends
show ipv6 traffic

Displays IPv6 traffic statistics.
show ipv6 traffic [if_name]

Syntax Definitions

if_name  Interface name. Restricts the display to the specified interface instead of global statistics.

Defaults

N/A.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The statistics show the cumulative totals since the last time the switch was powered on, the last reset of the switch was executed or the traffic statistics were cleared using the command.

Examples

-> show ipv6 traffic

<table>
<thead>
<tr>
<th>Message</th>
<th>Current</th>
<th>Previous</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets received</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>66193</td>
<td>0</td>
<td>66193</td>
</tr>
<tr>
<td>Header errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Too big</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>No route</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Address errors</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unknown protocol</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Truncated packets</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Local discards</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Delivered to users</td>
<td>969</td>
<td>0</td>
<td>969</td>
</tr>
<tr>
<td>Reassembly needed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Reassembly failed</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>66191</td>
<td>0</td>
<td>66191</td>
</tr>
</tbody>
</table>

Packets sent

|                  |         |          |        |
| Forwarded        | 0       | 0        | 0      |
| Generated        | 23      | 0        | 23     |
| Local discards   | 5       | 0        | 5      |
| Fragmented       | 0       | 0        | 0      |
| Fragmentation failed | 0     | 0        | 0      |
| Fragments generated | 0    | 0        | 0      |
| Multicast packets | 34      | 0        | 34     |
**output definitions**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>Total number of input packets received, including those received in error.</td>
</tr>
<tr>
<td>Header errors</td>
<td>Number of input packets discarded due to errors in their IPv6 headers (e.g., version number mismatch, other format errors, hop count exceeded, and errors discovered in processing their IPv6 options).</td>
</tr>
<tr>
<td>Too big</td>
<td>Number of input packets that could not be forwarded because their size exceeded the link MTU of the outgoing interface.</td>
</tr>
<tr>
<td>No route</td>
<td>Number of input packets discarded because no route could be found to transmit them to their destination.</td>
</tr>
<tr>
<td>Address errors</td>
<td>Number of input packets discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes).</td>
</tr>
<tr>
<td>Unknown protocol</td>
<td>Number of locally-addressed packets received successfully but discarded because of an unknown or unsupported protocol.</td>
</tr>
<tr>
<td>Truncated packets</td>
<td>Number of input packets discarded because the packet frame did not carry enough data.</td>
</tr>
<tr>
<td>Local discards</td>
<td>Number of input IPv6 packets for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any packets discarded while awaiting re-assembly.</td>
</tr>
<tr>
<td>Delivered to users</td>
<td>Total number of packets successfully delivered to IPv6 user protocols (including ICMP).</td>
</tr>
<tr>
<td>Reassembly needed</td>
<td>Number of IPv6 fragments received that needed to be reassembled.</td>
</tr>
<tr>
<td>Reassembly failed</td>
<td>Number of failures detected by the IPv6 reassembly algorithm (for whatever reason: timed out, errors, etc.).</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>Number of multicast packets received.</td>
</tr>
<tr>
<td>Forwarded</td>
<td>Number of output packets that this entity received and forwarded to their final destinations.</td>
</tr>
<tr>
<td>Generated</td>
<td>Total number of IPv6 packets that local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any packets counted by the Forwarded statistic.</td>
</tr>
<tr>
<td>Local discards</td>
<td>Number of output IPv6 packets for which no problem was encountered to prevent their transmission to their destination, but were discarded (e.g., for lack of buffer space). Note that this counter would include packets counted by the Forwarded statistic if any such packets met this (discretionary) discard criterion.</td>
</tr>
<tr>
<td>Fragmented</td>
<td>Number of IPv6 packets successfully fragmented.</td>
</tr>
<tr>
<td>Fragmentation failed</td>
<td>Number of IPv6 packets discarded because they needed to be fragmented but could not be.</td>
</tr>
<tr>
<td>Fragments generated</td>
<td>Number of output packet fragments generated as a result of fragmentation.</td>
</tr>
<tr>
<td>Multicast packets</td>
<td>Number of multicast packets transmitted.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 icmp statistics* Displays IPv6 ICMP statistics.

**MIB Objects**

`ipv6IfStatsTable`

- `ipv6IfStatsInReceives`
- `ipv6IfStatsInHdrErrors`
- `ipv6IfStatsInTooBigErrors`
- `ipv6IfStatsInNoRoutes`
- `ipv6IfStatsInAddrErrors`
- `ipv6IfStatsInUnknownProtos`
- `ipv6IfStatsInTruncatedPkts`
- `ipv6IfStatsInDiscards`
- `ipv6IfStatsInDelivers`
- `ipv6IfStatsOutForwDatagrams`
- `ipv6IfStatsOutRequests`
- `ipv6IfStatsOutDiscards`
- `ipv6IfStatsOutFragOKs`
- `ipv6IfStatsOutFragFails`
- `ipv6IfStatsOutFragCreates`
- `ipv6IfStatsReasmReqds`
- `ipv6IfStatsReasmOKs`
- `ipv6IfStatsReasmFails`
- `ipv6IfStatsInMcastPkts`
- `ipv6IfStatsOutMcastPkts`
show ipv6 tunnel configured

Displays IPv6 tunnel information and whether the 6to4 tunnel is enabled.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 tunnel configured

IPv6 6to4 tunnel: Enabled
Configured Tunnels:

<table>
<thead>
<tr>
<th>Tunnel</th>
<th>IPv6 Address/Prefix Length</th>
<th>Source IPv4</th>
<th>Destination IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2001:0000:0200::101/48</td>
<td>192.16.10.101</td>
<td>192.28.5.254</td>
</tr>
<tr>
<td>23</td>
<td>2001:0000:0200::102/48</td>
<td>192.15.10.102</td>
<td>10.27.105.25</td>
</tr>
<tr>
<td>v6if-tunnel-137</td>
<td>fe80::2d0:95ff:fe12:f470/64</td>
<td>212.35.35.35</td>
<td>212.104.138.137</td>
</tr>
</tbody>
</table>

Output definitions

IPv6 6to4 tunnel: Indicates whether 6to4 tunneling is enabled or disabled on the switch.
Tunnel: Tunnel ID.
IPv6 Address/Prefix Length: IPv6 address associated with the tunnel.
Source IPv4: Source IPv4 address for the tunnel.
Destination IPv4: Destination IPv4 address for the tunnel.
Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 interface

Configures an IPv6 interface on a VLAN or IPv6 tunnel.

MIB Objects

alaIPv6ConfigTunnelTable
  alaIPv6Tunnel6to4
  alaIPv6ConfigTunnelv4Source
  alaIPv6ConfigTunnelv4Dest
show ipv6 tunnel 6to4

Displays IPv6 tunnel information and whether the 6to4 tunnel is enabled.
show ipv6 tunnel 6to4

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples

-> show ipv6 tunnel 6to4
tunnel_6to4
   Status = Disabled
   IPv6 Address(es):
   Local IPv4 Address(es):

output definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>Indicates whether 6to4 tunneling is enabled or disabled on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Tunnel ID.</td>
</tr>
<tr>
<td>IPv6 Address(es)</td>
<td>IPv6 address associated with the tunnel.</td>
</tr>
<tr>
<td>Local IPv4 Addresses(es)</td>
<td>Source IPv4 address for the tunnel.</td>
</tr>
</tbody>
</table>

Release History
Release 7.1.1; command was introduced.
**Related Commands**

*ipv6 interface*  
Configures an IPv6 interface on a VLAN or IPv6 tunnel.

**MIB Objects**

alaIPv6ConfigTunnelTable

  - alaIPv6Tunnel6to4
  - alaIPv6ConfigTunnelv4Source
  - alaIPv6ConfigTunnelv4Dest
**show ipv6 udp ports**

Displays UDP Over IPv6 Listener Table. This table contains information about UDP/IPv6 endpoints.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only endpoints utilizing IPv6 addresses are displayed in this table.

**Examples**

`-> show ipv6 udp ports`

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Port</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>::</td>
<td>521</td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Local Port number for the UDP connection.</td>
</tr>
<tr>
<td>Interface</td>
<td>Name of the interface the listener is using or “unknown.”</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 routes*  
Displays TCP Over IPv6 Connection Table.

**MIB Objects**

IPv6UdpTable

IPv6UdpEntry  
IPv6UdpLocalAddress  
IPv6UdpLocalPort  
IPv6UdpIfIndex
# show ipv6 information

Displays IPv6 information.

## Syntax Definitions

N/A

## Defaults

N/A

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Usage Guidelines

N/A

## Examples

```
-> show ipv6 information
Default hop limit = 64
Path MTU entry minimum lifetime (min) = 10
Neighbor stale lifetime (min) = 10
Local Unicast Global ID = none
Use VRRP virtual source MAC = Off
Neighbor cache limit = None
VRF neighbor cache limit = None
Ignore anycast echo requests = No
Ignore multicast echo requests = No
ICMPv6 error rate limit interval (ms) = 10
ICMPv6 error rate limit burst = 10
```

## Output Definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Default hop limit</strong></td>
<td>The value placed in the hop limit field in router advertisements</td>
</tr>
<tr>
<td><strong>Path MTU entry minimum lifetime</strong></td>
<td>Minimum lifetime for entries in the path MTU.</td>
</tr>
<tr>
<td><strong>Neighbor stale lifetime</strong></td>
<td>Minimum lifetime for neighbor entries in the stale state.</td>
</tr>
<tr>
<td><strong>Local Unicast Global ID</strong></td>
<td>The default global ID value used in unique local unicast addresses.</td>
</tr>
<tr>
<td></td>
<td>&quot;none&quot; if a global ID has not been configured.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use VRRP virtual source MAC</td>
<td>If On, when a packet's source address is a VRRP virtual IPv6 address, the corresponding VRRP virtual MAC will be used as the source MAC address. If Off, the interface's real MAC will be used as the source MAC address.</td>
</tr>
<tr>
<td>Neighbor cache limit</td>
<td>The system-wide neighbor cache limit. If this value is not set: • “64” is displayed on the OmniSwitch 6465. • “128” is displayed on the OmniSwitch 6560 and OmniSwitch 6570M. • “none” is displayed on all other supported OmniSwitch platforms.</td>
</tr>
<tr>
<td>VRF neighbor cache limit</td>
<td>The neighbor cache limit in use for the VRF in which the command was executed. If this value is not set: • “64” is displayed on the OmniSwitch 6465. • “128” is displayed on the OmniSwitch 6560 and OmniSwitch 6570M. • “none” is displayed on all other supported OmniSwitch platforms.</td>
</tr>
<tr>
<td>Ignore anycast echo requests</td>
<td>States whether the echo reply to anycast echo request is set to Yes or No. If set to Yes, echo replies will not be sent in response to an echo request sent to an anycast address. If set to No, the switch will reply to all anycast echo requests.</td>
</tr>
<tr>
<td>Ignore multicast echo requests</td>
<td>States whether the echo reply to multicast echo request is set to Yes or No. If set to Yes, echo replies will not be sent in response to an echo request sent to a multicast address. If set to No, the switch will reply to all multicast echo requests.</td>
</tr>
<tr>
<td>ICMPv6 error rate limit interval</td>
<td>The rate limit interval in milliseconds.</td>
</tr>
<tr>
<td>ICMPv6 error rate limit burst</td>
<td>The maximum ICMPv6 error message burst size.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.4.1: ignore anycast echo requests, ignore multicast echo requests, ICMPv6 error rate limit interval, ICMPv6 error rate limit burst fields added.

Related Commands

ipv6 neighbor           | Configures a static entry in the IPv6 Neighbor Table.                                                                                             |
ipv6 pmtu-lifetime      | Configures the minimum lifetime for entries in the path MTU Table.                                                                               |
ipv6 hop-limit           | Configures the value placed in the hop limit field in the header of all IPv6 packet.                                                            |
ipv6 address global-id  | Configures the default global ID for unique local unicast addresses                                                                             |
ipv6 echo               | Configures the switch to reply or ignore echo requests in response to an echo request sent to a multicast or anycast IPv6 address.         |

MIB Objects

ipv6MibObjects
  IPv6DefaultHopLimit
  alaIPv6ConfigTable
    alaIPv6PMTUMinLifetime
    alaIPv6NeighborTable
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 information</code></td>
<td>Displays global IPv6 statistics and configuration.</td>
</tr>
</tbody>
</table>

`alaIPv6NeighborStaleLifetime`
ipv6 redist

Controls the conditions for redistributing IPv6 routes between different protocols.

```
ipv6 redist {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} {all-routes | route-map route_map_name} [admin-state {enable | disable}]
```

```
no ipv6 redist {local | static | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} {all-routes | route-map route_map_name}
```

---

**Syntax Definitions**

- **local**: Redistributes local IPv6 routes.
- **static**: Redistributes static IPv6 routes.
- **rip**: Specifies RIP as the source or destination (into) protocol.
- **ospf**: Specifies OSPF as the source or destination (into) protocol.
- **isis**: Specifies IS-IS as the source or destination (into) protocol.
- **bgp**: Specifies BGP as the source or destination (into) protocol.
- **import**: Redistributes imported routes to other routing protocols.
- **all-routes**: Redistributes all routes. This option does not allocate route-map resources.
- **route_map_name**: Name of an existing route map that will control the redistribution of routes between the source and destination protocol.
- **enable**: Enables the administrative status of the redistribution configuration.
- **disable**: Disables the administrative status of the redistribution configuration.

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T48C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to remove a route map redistribution configuration. Note that if a route map name is not specified, all route maps associated with the redistribution configuration are removed.
- The source and destination protocols must be loaded and enabled before redistribution occurs.
- The IPv6 version of BGP is not supported in the current release.
- Use the `ip route-map` commands described in the “IP Commands” chapter of this guide to create a route map. Refer to the “Configuring IP” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about how to create a route map.

**Examples**

```
-> ipv6 redist rip into ospf route-map rip-to-ospf1
-> ipv6 redist rip into ospf route-map rip-to-ospf2
-> no ipv6 redist rip into ospf route-map rip-to-ospf2
-> ipv6 redist local into rip route-map local-to-rip
-> ipv6 redist local into rip route-map local-to-rip disable
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.2; `all-routes` parameter added.
Release 8.5R1; `import` parameter added.

**Related Commands**

- `show ipv6 redist` Displays the route map redistribution configuration.

**MIB Objects**

- `alaRouteMapRedistProtoTable`
- `alaRouteMapRedistSrcProtoId`
- `alaRouteMapRedistDestProtoId`
- `alaRouteMapRedistRouteMapIndex`
- `alaRouteMapRedistStatus`
- `alaRouteMapRedistAddressType`
- `alaRouteMapRedistRowStatus`
ipv6 access-list

Creates an IPv6 access list that is used to specify multiple IPv6 addresses for a route map configuration.

ipv6 access-list access_list_name

no ipv6 access-list access_list_name

Syntax Definitions

access_list_name Name of the IPv6 access list (up to 20 characters).

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the no form of this command to delete the access list.

Examples

- -> ipv6 access-list access1
- -> no ipv6 access-list access1

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 access-list address Adds IPv6 addresses to an existing IPv6 access list.

show ipv6 access-list Displays the contents of an IPv6 access list.

MIB Objects

alaRouteMapAccessListNameTable
alaRouteMapAccessListName
alaRouteMapAccessListNameIndex
alaRouteMapAccessListNameAddressType
**ipv6 access-list address**

Adds IPv6 addresses to the specified IPv6 access list.

```
ipv6 access-list access_list_name address address/prefixLen [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
```

```
no ipv6 access-list access_list_name address address/prefixLen
```

---

### Syntax Definitions

- **access_list_name**: Name of the IPv6 access list (up to 20 characters).
- **address/prefixLen**: IPv6 address along with the prefix length to be added to the access list.
- **permit**: Permits the IPv6 address for redistribution.
- **deny**: Denies the IPv6 address for redistribution.
- **all-subnets**: Redistributes or denies all the subnet routes that match the network portion of the IP address as specified by the mask length.
- **no-subnets**: Redistributes or denies only those routes that exactly match the IP address and the mask length.
- **aggregate**: Redistributes an aggregate route if there are one or more routes that match or are subnets of this address.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
<tr>
<td>all-subnets</td>
<td>no-subnets</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to delete the address from the access list.
- The `access_list_name` should exist before you add multiple IPv6 addresses to the IPv6 access list.
- The `action` parameters (perm [mit and deny]) determine if a route that matches the `redist-control` configuration for the IP address is allowed or denied redistribution.
- The `redist-control` parameters (all-subnets, no-subnets, and aggregate) defines the criteria used to determine if a route matches an address in the access list.

- Note that configuring the combination of `redist-control aggregate` with `action deny` is not allowed.

- Use this command multiple times with the same access list name to add multiple addresses to the existing IPv6 access list.

**Examples**

```
-> ipv6 access-list access1 address 2001::1/64 action permit
-> ipv6 access-list access1 address 2001::1/64 redist-control aggregate
-> no ipv6 access-list access1 address 2001::1/64
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ipv6 access-list` Creates an IPv6 access list that is used to specify multiple IPv6 addresses for a route map configuration.

- `show ipv6 access-list` Displays the contents of an IPv6 access list.

**MIB Objects**

alaRouteMapAccessListTable
  alaRouteMapAccessListIndex
  alaRouteMapAccessListAddress
  alaRouteMapAccessListAddressType
  alaRouteMapAccessListPrefixLength
  alaRouteMapAccessListAction
  alaRouteMapAccessListRedistControl
  alaRouteMapAccessListRowStatus
show ipv6 redist

Displays the IPv6 route map redistribution configuration.

show ipv6 redist [rip | ospf | bgp]

**Syntax Definitions**

- **rip**
  Displays the route map redistribution configurations that specify RIP as the destination (into) protocol.

- **ospf**
  Displays the route map redistribution configurations that specify OSPF as the destination (into) protocol.

- **bgp**
  Displays the route map redistribution configurations that specify BGP as the destination (into) protocol.

**Defaults**

By default all route map redistribution configurations are shown.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify a destination protocol with this command to display only those configurations that redistribute routes into the specified protocol.

- The IPv6 version of BGP is not supported in the current release.

**Release History**

Release 7.1.1; command was introduced.

**Examples**

```
-> show ipv6 redist

Source       Destination  Status    Route Map
Protocol     Protocol     
------------+------------+---------+-------------------
localIPv6    RIPng       Enabled   ipv6rm
RIPng        OSPFv3      Enabled   ipv6rm
```
-> show ipv6 redist ospf

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Protocol</th>
<th>Status</th>
<th>Route Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIPng</td>
<td>OSPFv3</td>
<td>Enabled</td>
<td>ipv6rm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

- **Source Protocol**: The protocol from which the routes are learned.
- **Destination Protocol**: The protocol into which the source protocol routes are redistributed.
- **Status**: The administrative status (Enabled or Disabled) of the route map redistribution configuration.
- **Route Map**: The name of the route map that is applied with this redistribution configuration.

**Related Commands**

- **ipv6 redist**: Controls the conditions for redistributing IPv6 routes between different protocols.
- **show ipv6 redist-routes**: Displays all of the IPv6 routes that have been redistributed.

**MIB Objects**

- alaRouteMapRedistProtoTable
  - alaRouteMapRedistSrcProtoId
  - alaRouteMapRedistDestProtoId
  - alaRouteMapRedistRouteMapIndex
  - alaRouteMapRedistStatus
  - alaRouteMapRedistAddressType
  - alaRouteMapRedistRowStatus
**show ipv6 redist-routes**

Displays all of the IPv6 routes that have been redistributed.

```
[vrf vrf_name] show ipv6 redist-routes
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `show ipv6 redist` command to display the IPv6 route redistribution configuration.

### Examples

```
-> show ipv6 redist-routes
Route Map  Route          Gateway    Source   Dest Metric RtType Tag    LocalPref Community
---------------------------------------------------------------------------------------------------------
None        1601::/16      1701::2    OSPF     RIP       5 INT        0
BgpMap      1801:1::/32    1901::2    OSPF     BGP       1 EXT        0         10 no-export
```

### output definitions

- **Route Map**: The name of the route map that is applied with this redistribution configuration.
- **Route**: The redistributed route.
- **Gateway**: IPv6 address of the gateway on which this route was learned.
- **Source**: The source protocol.
- **Dest**: The destination protocol.
- **Metric**: RIP metric or cost (hop count) for the route. Indicates a priority for the route. The lower the metric value, the higher the priority.
show ipv6 redist-routes

output definitions

RtType  The type of route:
  • NONE—No route type.
  • INTERNAL—OSPF/BGP internal routes.
  • EXTERNAL—OSPF/BGP external routes.
  • TYPE1—OSPF external Type-1 routes.
  • TYPE2—OSPF external Type-2 routes.
  • LEVEL1—IS-IS Level-1 routes only.
  • LEVEL2—IS-IS Level-2 routes only.

Tag  The tag value of the route.

LocalPref  The local route preference of a route being redistributed into BGP.

Community  The community name of a route being redistributed into BGP.

Release History

Release 8.4.1.R03; command introduced.

Related Commands

ipv6 redist  Controls the conditions for redistributing different IPv4 routes between protocols.

show ipv6 redist  Displays the route map redistribution configuration.

MIB Objects

N/A
**show ipv6 access-list**

Displays the contents of the specified IPv6 access list.

**show ipv6 access-list** [access_list_name]

---

**Syntax Definitions**

access_list_name  
Name of the IPv6 access list.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6865N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

If the *access_list_name* is not specified in this command, all the access lists will be displayed.

---

**Examples**

```
-> show ipv6 access-list

<table>
<thead>
<tr>
<th>Name</th>
<th>Address / Prefix Length</th>
<th>Redistribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>al_3</td>
<td>128::/64</td>
<td>permit all-subnets</td>
</tr>
<tr>
<td>al_4</td>
<td>124::/64</td>
<td>permit no-subnets</td>
</tr>
</tbody>
</table>
```

```
-> show ipv6 access-list 4

<table>
<thead>
<tr>
<th>Name</th>
<th>Address / Prefix Length</th>
<th>Redistribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>al_4</td>
<td>124::/64</td>
<td>permit no-subnets</td>
</tr>
</tbody>
</table>
```

---

**output definitions**

- **Name**: Name of the IPv6 access list.
- **Address/Prefix Length**: IPv6 address that belongs to the access list.
output definitions

| Effect | Indicates whether the IPv6 address is permitted or denied for redistribution. |
| Redistribution Control | Indicates the conditions specified for redistributing the matched routes. |

Release History

Release 7.1.1; command was introduced

Related Commands

ipv6 access-list

Creates an IPv6 access list for adding multiple IPv6 addresses to route maps.

ipv6 access-list address

Adds multiple IPv6 addresses to the IPv6 access list.

MIB objects

alaRouteMapAccessListIndex
alaRouteMapAccessListAddressType
alaRouteMapAccessListAddress
alaRouteMapAccessListPrefixLength
alaRouteMapAccessListAction
alaRouteMapAccessListRedistControl
### ipv6 export

Exports IPv6 routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances. All routes are exported or a route map can be specified to filter exported routes.

```
[vrf vrf_name] ipv6 export {all-routes | route-map route_map_name | to-all-vrfs {all-routes | route-map route_map_name}}
```

```
[vrf vrf_name] no ipv6 export
```

#### Syntax Definitions

- **vrf_name**
  - The name of an existing VRF instance. Routes are exported from this source VRF to the GRT.

- **all-routes**
  - Exports all routes from the source VRF to the GRT. This option does not allocate route-map resources.

- **route_map_name**
  - The name of an existing route-map to use for filtering routes that are exported from the source VRF to the GRT.

- **to-all-vrfs all-routes**
  - Exports all routes to all of the other VRF instances, except to VRFs that already have an import configured for the source (export) VRF.

- **to-all-vrfs route-map route_map_name**
  - The name of an existing route map to use for filtering routes that are exported from the source VRF to all other VRF instances.

#### Defaults

- If a source VRF name is not specified with this command, routes are exported from within the context of the active VRF instance to the GRT.

- If there are no VRF instances configured on the switch, the routes are exported from the default VRF to the GRT.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- Use the **no** form of this command to disable exporting of routes from the VRF to GRT.

- To leak IPv6 routes between VRF instances, IPv6 must be available in both instances. It is important to note that IPv6 route leaking is supported only in max profile VRFs.

- IPv6 route leaking supports configured tunnel routes, but 6to4 tunnel and loopback routes are not supported.
• Routes that were leaked into a VRF instance cannot be exported from that instance to another VRF.

• The route map name specified with this command must already exist in the switch configuration. See the \texttt{ip route-map} commands in the “IP Commands” chapter of this guide and the “Configuring IP” chapter in the \emph{OmniSwitch AOS Release 8 Network Configuration Guide} for more information about how to create a route map.

• A route map created to filter exported VRF IPv6 routes can contain any of the following match and set options:
  – Match options: ipv6-address, ipv6-next-hop, tag, protocol, ipv6-interface, metric, route-type, name
  – Set options: tag, metric

• A route map with redist control of aggregate is supported when exporting IPv6 routes, but it is not supported when importing IPv6 routes.

• Only one route map per source VRF is allowed for filtering exported routes.

• Only those FDB (Forwarding Routing Database) routes that match the conditions of the route map are exported to GRT.

• Modifying a route map that is assigned to a VRF through the \texttt{ipv6 import} or \texttt{ipv6 export} command is supported.

\textbf{Examples}

The following commands export IPv6 routes from the current VRF routing table (or from the default VRF if there are no other VRFs configured) to the GRT:

\begin{verbatim}
-> ipv6 export route-map R1
-> ipv6 export all-routes
-> ipv6 export to-all-vrfs all-routes
-> ipv6 export to-all-vrfs route-map R2
-> no ipv6 export
\end{verbatim}

The following commands export IPv6 routes from the “vrf2” routing table to the GRT even though the command line is operating within the context of the default VRF instance:

\begin{verbatim}
-> vrf vrf2 ipv6 export route-map R1
-> vrf vrf2 ipv6 export all-routes
-> vrf vrf2 ipv6 export to-all-vrfs all-routes
-> vrf vrf2 ipv6 export to-all-vrfs route-map R2
-> no vrf vrf2 ipv6 export
\end{verbatim}

The following commands first change the command line context to the “vrf1” instance so that all subsequent commands export routes from “vrf1” without having to specify the VRF name with each command:

\begin{verbatim}
-> vrf vrf1
vrf1::-> ipv6 export route-map R1
vrf1::-> ipv6 export all-routes
vrf1::-> ipv6 export to-all-vrfs all-routes
vrf1::-> ipv6 export to-all-vrfs route-map R2
vrf1::-> no ipv6 export
\end{verbatim}

\textbf{Release History}

Release 8.5R1; command introduced.
**Related Commands**

- **vrf**
  Configures and selects a virtual routing and forwarding (VRF) instance on the switch.

- **ip route-map action**
  Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

- **ip route-map match protocol**
  Matches the protocol specified in the route map with the protocol of the route.

- **show ipv6 export**
  Displays the export route configuration details.

- **show ipv6 global-route-table**
  Displays the GRT for all the routes that are exported from the VRFs.

- **show ip route-map**
  Displays the configured IP route maps.

**MIB Objects**

- aIprmV6ExportRouteMap
- aIprmV6ExportToAllVrfsRouteMap
**ipv6 import**

Imports VRF IPv6 routes from the GRT to the destination VRF. All routes are imported or a route map can be specified to filter imported routes.

```
[vrf dest_vrf_name] ipv6 import {vrf {src_vrf_name | default} | isid instance_id} {all-routes | route-map route_map_name}

[vrf dest_vrf_name] no ipv6 import vrf {src_vrf_name | default}
```

---

**Syntax Definitions**

- **dest_vrf_name**: The name of the destination VRF instance into which routes are imported from the GRT.
- **src_vrf_name**: The name of the source VRF instance from which routes were exported to the GRT. Routes from this instance are imported from the GRT into the specified destination VRF instance.
- **default**: Default VRF. The routes are imported from the default VRF instance.
- **instance_id**: An existing ISID number that identifies an SPB service in a provider backbone bridge (PBB) network. The routes for this ISID number are imported from the GRT into the current or specified VRF instance.
- **all-routes**: Imports all routes from the source VRF instance. Imported routes are not filtered.
- **route_map_name**: The name of an existing route map to use for filtering routes that are imported from the GRT to the destination VRF. Imported routes are filtered based on the options defined in the route map.

---

**Defaults**

If a destination VRF name is not specified with this command, routes are imported from the GRT into the context of the active VRF instance.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
</tr>
<tr>
<td>6560</td>
<td>6570M</td>
</tr>
<tr>
<td>6860</td>
<td>6860N</td>
</tr>
<tr>
<td>6900</td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td></td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td></td>
</tr>
<tr>
<td>6900 C32E/T24C2/</td>
<td></td>
</tr>
<tr>
<td>6900 X24C2</td>
<td></td>
</tr>
</tbody>
</table>

| 9900 |                        |

---

**Usage Guidelines**

- Use the **no** form of this command to remove the IP import routes configuration for the specified VRF or ISID instance.
- To leak IPv6 routes between VRF instances, IPv6 must be available in both instances. It is important to note that IPv6 route leaking is supported only in max profile VRFs.
• IPv6 route leaking supports configured tunnel routes, but 6to4 tunnel and loopback routes are not supported.

• Routes that were leaked into a VRF instance cannot be exported from that instance to another VRF.

• The route map name specified with this command must already exist in the switch configuration. See the ip route-map commands in the “IP Commands” chapter of this guide and the “Configuring IP” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide for more information about how to create a route map.

• A route map created to filter imported VRF or ISID IPv6 routes can contain any of the following match and set parameter options:
  – Match options: ipv6-address (no aggregates), ipv6-next-hop, tag, metric
  – Set options: tag, metric

• A route map with redist control of aggregate is supported when exporting IPv6 routes, but it is not supported when importing IPv6 routes.

• Only one route map per source (imported) VRF or ISID is allowed.

• Modifying a route map that is assigned to a VRF or ISID through the ipv6 import or ipv6 export command is supported.

• Leaked routes are only for forwarding. If a local route is leaked, that interface is not accessible in the importing VRF. Another switch will not be able to ping the interface in the import VRF.

Examples

-> ipv6 import vrf V1 route-map R2
-> ipv6 import vrf V2 all-routes
-> no ipv6 import vrf V1

-> vrf V3 ipv6 import vrf V2 route-map import-map
-> vrf V3 no ipv6 import vrf V2

-> ipv6 import isid 1500 route-map R1
-> ipv6 import isid 2000 all-routes
-> no ipv6 import isid 1500

-> vrf V4 ipv6 import isid 2500 route-map import-map
-> vrf V4 no ipv6 import isid 2500

Release History

Release 8.5R1; command introduced.
Release 8.5R2; isid parameter added.
**Related Commands**

**vrf**
Configures and selects a virtual routing and forwarding (VRF) instance on the switch.

**ip route-map action**
Creates a route map for selecting or filtering routes for tasks such as redistribution and VRF route leaking. It also sets the action of the route map to permit or deny.

**ip route-map match protocol**
Matches the protocol specified in the route map with the protocol of the route.

**show ipv6 import**
Displays the import route configuration details.

**show ipv6 global-route-table**
Displays the GRT for all the routes that are exported from the VRFs.

**show ip route-map**
Displays the configured IP route maps.

**MIB Objects**

`alaIprmV6ImportVrfTable`

`alaIprmV6ImportVrfName`

`alaIprmV6ImportVrfRouteMap`

`alaIprmV6ImportISid`

`alaIprmV6ImportVrfRowStatus`
show ipv6 export

Displays the export route configuration details.

[vrf vrf_name] show ipv6 export

Syntax Definitions

vrf_name The name of an existing VRF instance.

Defaults

By default, the export route configuration for the active VRF instance is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If a VRF is specified, the export route configuration for that VRF is displayed.

Examples

-> show ipv6 export
Export Route Map: leak-out

-> vrf vrf1 show ipv6 export
Export Route Map: none (all-routes)

vrf2:-> show ipv6 export
Export Route Map: none (all-routes) -> To All VRFs

Release History

Release 8.5R1; command introduced.
**Related Commands**

**ipv6 export**

Exports IPv6 routes from the source VRF to the Global Routing Table (GRT) or to all VRF instances.

**MIB Objects**

alaIprmV6ExportRouteMap
alaIprmV6ExportToAllVrfsRouteMap
show ipv6 import

Displays the import route configuration details.

[vrf vrf_name] show ipv6 import

Syntax Definitions

vrf_name

The name of an existing VRF instance.

Defaults

By default, the import route configuration for the active VRF instance is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If a VRF is specified, the import route configuration for that VRF is displayed.

Examples

-> show ipv6 import
Type Source RouteMap
-----------------------------+-----------------------------
vrf Customer1 leak-in
vrf Customer2 none (all-routes)
isid 1000 isid1000-filter

output definitions

<table>
<thead>
<tr>
<th>Type</th>
<th>The type of imported route (vrf or isid).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The name of the VRF instance from which IPv6 routes are imported to the VRF.</td>
</tr>
<tr>
<td>RouteMap</td>
<td>The name of the route map filter or none (all-routes).</td>
</tr>
</tbody>
</table>

Release History

Release 8.5R1; command introduced.
Release 8.5R2; imported ISID route entries added to the table.
**Related Commands**

`ipv6 import`  
Imports VRF IPv6 routes from the GRT to the destination VRF.

**MIB Objects**

`alaIprmV6ImportVrfTable`
- `alaIprmV6ImportVrfName`
- `alaIprmV6ImportIsid`
- `alaIprmV6ImportVrfRouteMap`
- `alaIprmV6ImportIsidRouteMap`
- `alaIprmV6ImportVrfRowStatus`
**show ipv6 global-route-table**

Displays the contents of the Global Routing Table (GRT) for all the IPv6 routes that are exported from VRF or from Shortest Path Bridging service instance identifiers (ISIDs). This command is only available within the context of the default VRF instance.

**show ipv6 global-route-table [export-vrf vrf_name]**

---

### Syntax Definitions

**vrf_name**

The alphanumeric name (1–20 characters) assigned to the VRF instance.

---

### Defaults

By default, exported routes are displayed for all VRF instances and ISIDs.

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

Use the `export-vrf` parameter to display exported routes for a specific VRF instance.

---

### Examples

```
-> show ipv6 global-route-table
```

<table>
<thead>
<tr>
<th>Type</th>
<th>Source</th>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
<th>Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Customer2</td>
<td>1601::/16</td>
<td>1701:ffff:0001::1</td>
<td>1</td>
<td>100</td>
</tr>
<tr>
<td>vrf</td>
<td>Customer2</td>
<td>1111::/16</td>
<td>1111::1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>vrf</td>
<td>Customer3</td>
<td>2808:3456::/32</td>
<td>3939::2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>isid</td>
<td>1000</td>
<td>1801::/16</td>
<td>2222::2</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

---

### output definitions

- **Type**: The type of exported route (vrf or isid).
- **Source**: The name of the VRF instance or the Shortest Path Bridging service instance identifier (ISID) from which IPv6 routes are exported to the GRT.
- **Destination**: The address of the route.
- **Gateway**: The next hop for the destination address.
- **Metric**: The metric of the exported route.
- **Tag**: The tag of the exported route.
**Release History**

Release 8.5R1; command introduced.
Release 8.5R2; exported ISID route entries added to the table.

**Related Commands**

`ipv6 export`  
Configures a route map to export routes from the source VRF to Global Routing Table (GRT).

`show ipv6 export`  
Displays the export route configuration details.

**MIB Objects**

alaGrt6RouteTable  
alaGrt6RouteDistinguisher  
alaGrt6RouteDest  
alaGrt6RouteMaskLen  
alaGrt6RouteNextHop  
alaGrt6RouteMetric  
alaGrt6RouteTag  
alaGrt6GrtVrfName  
alaGrt6RouteIsid
22 IPsec Commands

IPsec is a suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream. IPsec provides security services such as Encrypting traffic, Integrity validation, Authenticating the peers, and Anti-replay.

IPsec protocols operate at network layer using appropriate security protocols, cryptographic algorithms, and cryptographic keys. The security services are provided through use of two security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols.

There are two modes of IPsec operation: transport mode and tunnel mode. In transport mode, only the data you transfer (payload) in the IP packet is encrypted and/or authenticated and only the payloads that are originated and destined between two intermediate systems are processed with IPsec. In tunnel mode, the entire IP packet with both the data and the message headers is encrypted and/or authenticated. In tunnel mode, all the IP packets that pass through the endpoints are processed by IPsec. The current implementation of IPsec supports only the transport mode.

The pre-configured Security Policy determines the traffic that is to be rendered with IPsec protection. A Security Association (SA) specifies the actual IPsec actions to be performed (e.g. encryption using 3DES, authentication with HMAC-SHA1). A security association is bundle of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. Security Associations can be manually configured or negotiated through IKE. The current implementation of IPsec does not support the negotiation of SA through IKE and SAs need to be configured manually.

Note. In the current implementation IPv4 supports only management service.

<table>
<thead>
<tr>
<th>Filename: ALCATEL-IND1-IPSEC-MIB.mib</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module: alcatelIND1IPsecMIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:

```
ipsec key
ipsec security-key
ipsec policy
ipsec policy rule
ipsec sa
ipsec default-discard
show ipsec policy
show ipsec sa
show ipsec key
show ipsec statistics
```
**ipsec key**

Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

```
ipsec key name {sa-authentication | sa-encryption} [encrypted] key
no ipsec key name {sa-authentication | sa-encryption}
```

---

**Syntax Definitions**

- **name**: The name of this key (maximum 20 characters).
- **sa-authentication**: Indicates that the key value is used for Authentication Header.
- **sa-encryption**: Indicates that the key value is used for Encapsulated Security Payload.
- **encrypted**: Not user configured, used only by switch in config file.
- **key**: Specifies the key value. The key value can be either in the hexadecimal format or as a string.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The **name** parameter must be same as the name of the manually configured SA that uses this SA authentication and encryption key.

- The length of the key value must match the value that is required by the encryption or authentication algorithm that uses the key. The required key length for the supported algorithm are as follows:

<table>
<thead>
<tr>
<th>algorithm</th>
<th>key length</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des-cbc</td>
<td>192 bits</td>
</tr>
<tr>
<td>aes-cbc</td>
<td>128, 192, or 256 bits</td>
</tr>
<tr>
<td>hmac-md5</td>
<td>128 bits</td>
</tr>
<tr>
<td>hmac-sha1</td>
<td>160 bits</td>
</tr>
<tr>
<td>hmac-sha2 -256</td>
<td>256 bits</td>
</tr>
<tr>
<td>hmac-sha2-384</td>
<td>384 bits</td>
</tr>
</tbody>
</table>
The combination of the key's name and type must be unique.

The encrypted option is used when the key commands are written to the boot.cfg or other snapshot file. This option can not be specified by the user when entering CLI commands.

**Examples**

```
-> ipsec key sa_md5_in sa-authentication takd03c9@skL68L%
```

**Release History**

Release 7.1.1; command introduced.
Release 8.7 R1; HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512 algorithm support for authentication added.

**Related Commands**

- **ipsec sa**
  Adds, modifies, or deletes a manually configured IPsec Security Association (SA).

- **show ipsec key**
  Displays the keys for the manually configured IPsec SA.

**MIB Objects**

AlaIPsecKeyTable
  - alaIPsecKeyName
  - alaIPsecKeyType
  - alaIPsecKeyEncrypted
  - alaIPsecKey

<table>
<thead>
<tr>
<th>algorithm</th>
<th>key length</th>
</tr>
</thead>
<tbody>
<tr>
<td>hmac-sha2-512</td>
<td>512 bits</td>
</tr>
<tr>
<td>aes-xcbc-mac</td>
<td>128</td>
</tr>
</tbody>
</table>
**ipsec security-key**

Sets the master security key for the switch. The master security key is used to encrypt and decrypt the configured SA keys.

```
ipsec security-key [old_key] new_key
```

### Syntax Definitions

- **old_key**: The current master security key. The key can be specified either in the hexadecimal format or as a string.
- **new_key**: The new key value. The key can be specified either in the hexadecimal format or as a string.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The `old_key` parameter must always be specified when you modify an existing key. Setting the key for first time does not require the `old_key`.
- If the value of the `old_key` is incorrect, the attempt to set a new key fails.
- While the SA keys can be configured without a master security key; the configured SA keys are written to the configuration file unencrypted, and a warning is logged.
- The security key must be 16 characters or 16 bytes if in hex form (32 hex digits).
- If the master security key is reset using `debug clear ipsec security-key` command, the currently configured SA keys are deleted.

### Examples

```
-> ipsec security-key "old key value ab" 0xa38d901bde77af091a2485ce0a14a8cc
```

### Release History

Release 7.1.1; command introduced.
Related Commands

**ipsec key**  
Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

MIB Objects

**AlaIPsecSecurityKeyTable**
- **alaIPsecSecurityKeyCurrent**
- **alaIPsecSecurityKeyNew**
ipsec policy

Adds, modifies, or removes a security policy.

```
ipsec policy name [service {telnet | ftp | ssh | snmp | http | https}] [priority priority] [source {ipv6_address[/prefix_length] | ipv4_address[/prefix_length]}] [source port] [destination {ipv6_address[/prefix_length] | ipv4_address[/prefix_length]}] [destination port] [protocol {any | icmp6 [type type] | tcp | udp | ospf | vrrp | number protocol}] [in | out] [discard | ipsec | none] [description description] [admin-state {enable | disable}]
```

no ipsec policy name

---

**Syntax Definitions**

- **name**: The name for the policy.
- **service**: The management service. This can be specified to restrict the policy to traffic from a specific service.
- **priority**: The priority for the policy. Values may range from 1 to 1000. The lower the value, the higher the priority.
- **source**: Specifies the source address of the IPv6 or IPv4 traffic that is covered by the policy.
- **source /prefix_length**: Specifies the prefix length of the source address of the IPv6 or IPv4 traffic that is covered by the policy.
- **source port**: Specifies the source port of the IPv6 traffic that is covered by the policy. The value 0 can be specified to match packets originated from any port.
- **destination**: Specifies the destination address of the IPv6 or IPv4 traffic that is covered by the policy.
- **destination /prefix-length**: Specifies the prefix length of the destination address of the IPv6 or IPv4 traffic that is covered by the policy.
- **destination port**: Specifies the destination port of the IPv6 or IPv4 traffic that is covered by the policy. The value 0 can be specified to match packets destined to any port.
- **protocol**: Specifies that the particular protocol specific traffic to be covered by the policy (Refer to the table in the “Usage Guidelines” section below for various protocol options). This option is supported only for IPv4 traffic on the management service.
- **in**: Specifies that the policy is applied to the inbound IPv6 or IPv4 traffic.
- **out**: Specifies that the policy is applied to the outbound IPv6 or IPv4 traffic.
- **discard**: Specifies the policy to discard the IPv6 or IPv4 packet, if it matches the criteria.
- **ipsec**: Specifies the policy to send the IPv6 or IPv4 packet for IPsec processing, if it matches the criteria.
- **none**: Specifies IPsec should not process the packet.
- **description**: The detailed description of the policy.
- **enable**: Administratively enables the policy.
- **disable**: Administratively disables the policy.
**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>100</td>
</tr>
<tr>
<td>port</td>
<td>0</td>
</tr>
<tr>
<td>any</td>
<td>icmp6</td>
</tr>
<tr>
<td>icmp6 type</td>
<td>not present</td>
</tr>
<tr>
<td>discard</td>
<td>ipsec</td>
</tr>
<tr>
<td>admin-state</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- If two policies can cover the same traffic, the policy with the highest priority is applied. If two policies have the same priority, the one configured first has precedence.

- The following table lists the various protocol options in this command:

<table>
<thead>
<tr>
<th>protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
</tr>
<tr>
<td>icmp6[type type]</td>
</tr>
<tr>
<td>tcp</td>
</tr>
<tr>
<td>udp</td>
</tr>
<tr>
<td>ospf</td>
</tr>
<tr>
<td>vrrp</td>
</tr>
<tr>
<td>number protocol</td>
</tr>
</tbody>
</table>

The any option must be used to apply the policy to all protocol traffic. Otherwise, an upper-layer protocol (or protocol number) may be specified to restrict the policy to the specified protocol traffic. The optional type parameter of icmp6 can also be specified to restrict the policy for certain type of ICMPv6 packets.

- If the ipsec option is specified this policy cannot be enabled until at least one rule has been defined. The policy rules specify that IPsec algorithms be applied to the traffic that matches the policy.
**Examples**

-> ipsec policy tcp_out source 2001:db8:3::12 destination 201:db8:4::a3e protocol tcp out ipsec description "Outbound TCP traffic" admin-state disable

-> ipsec policy tcp_out source 10.20.1.2 destination 10.20.10.1 protocol tcp out ipsec description "Outbound TCP traffic" admin-state disable

-> no ipsec policy tcp_out

**Release History**

Release 7.1.1; command introduced.
Release 8.7 R1; IPv4 support added.

**Related Commands**

- **ipsec policy rule**  
  Adds, modifies, or removes an IPsec rule for a security policy.

- **show ipsec policy**  
  Displays information about the security policies.

**MIB Objects**

AlaIPsecSecurityPolicyTable
  alaIPsecSecurityPolicyName  
  alaIPsecSecurityPolicyPriority  
  alaIPsecSecurityPolicySource  
  alaIPsecSecurityPolicySourceType  
  alaIPsecSecurityPolicySourcePrefixLength  
  alaIPsecSecurityPolicySourcePort  
  alaIPsecSecurityPolicyDestination  
  alaIPsecSecurityPolicyDestinationType  
  alaIPsecSecurityPolicyDestinationPrefixLength  
  alaIPsecSecurityPolicyDestinationPort  
  alaIPsecSecurityPolicyULProtocol  
  alaIPsecSecurityPolicyICMPv6Type  
  alaIPsecSecurityPolicyDirection  
  alaIPsecSecurityPolicyAction  
  alaIPsecSecurityPolicyDescription  
  alaIPsecSecurityPolicyAdminState
ipsec policy rule

Adds, modifies, or removes an IPsec rule for a security policy.

```
ipsec policy name rule index [ah | esp]
no ipsec policy name
```

Syntax Definitions

- **name**: The name of the security policy created by using the `ipsec policy` command.
- **index**: The index of this rule. Values may range from 1 to 10.
- **ah**: Specifies that the rule requires the presence of an Authentication Header (AH).
- **esp**: Specifies that the rule requires the presence of an Encrypted Security Payload header (ESP).

Defaults

N/A.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `index` parameter to specify the order in which the multiple rules for the same security policy are applied to the original payload.

Examples

```
-> ipsec policy alucent rule 1 ah
-> no ipsec policy alucent
```

Release History

Release 7.1.1; command introduced.
**Related Commands**

**ipsec policy**

Adds, modifies, or removes a security policy.

**MIB Objects**

`AlaIPsecSecurityPolicyRuleTable`

- `alaIPsecSecurityPolicyName`
- `alaIPsecSecurityPolicyRuleIndex`
- `alaIPsecSecurityPolicyRuleProtocol`
**ipsec sa**

Adds, modifies, or deletes a manually configured IPsec Security Association (SA).

```
ipsec sa name {esp | ah} [source {ipv6_address | ipv4_address}] [destination {ipv6_address | ipv4_address}] [spi spi] [encryption {null | 3des-cbc | aes-cbc [key-size key_length]}] [authentication {none | hmac-md5 | hmac-sha1 | hmac-sha256 | hmac-sha384 | hmac-sha512 | aes-xcbc-mac}] [description description] [admin-state {enable | disable}]
```

**no ipsec sa name**

---

**Syntax Definitions**

- **name**
  - The name assigned to this IPsec SA.

- **esp**
  - Specifies the type of security association as ESP.

- **ah**
  - Specifies the type of security association as AH.

- **source**
  - Specifies the source address of the IPv6 or IPv4 traffic that is covered by the SA.

- **destination**
  - Specifies the destination address of the IPv6 or IPv4 traffic that is covered by the SA.

- **spi**
  - The Security Parameters Index (SPI) for the SA.

- **encryption**
  - Specifies the encryption algorithm to be used for traffic covered by the SA. This parameter must be used only when the SA type is ESP.

- **key_length**
  - Key length for the specified encryption algorithm.

- **authentication**
  - Specifies the authentication algorithm to be used for traffic covered by the SA.

- **description**
  - The detailed description of the SA.

- **enable**
  - Administratively enables the SA.

- **disable**
  - Administratively disables the SA.
### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>encryption</td>
<td>none</td>
</tr>
<tr>
<td>authentication</td>
<td>none</td>
</tr>
<tr>
<td>admin-state</td>
<td>enable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The `encryption` parameter must be specified with the `none` option, if ESP is being used to verify integrity only.

- If `null` is specified as the option for `encryption`, an integrity algorithm must be specified using the `authentication` parameter.

- To override a default key length in an `encryption` algorithm, the key length must be specified after the protocol name. The key length supported for various algorithm are as follows:

<table>
<thead>
<tr>
<th>encryption algorithm</th>
<th>key length (in bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes-cbc</td>
<td>128 (default), 192, and 256</td>
</tr>
</tbody>
</table>

- For AH SAs, one of the authentication algorithms such as aes-xcbc-mac, hmac-md5 or hmac-sha1 must be specified.

### Examples

```bash
-> ipsec sa esp_in_1 esp source 2001:db8:3::13d destination 2001:db8:1::24 spi 10392 encryption aes-cbc authentication hmac-sha1
-> no ipsec sa esp_in_1
```

### Release History

Release 7.1.1; command introduced.
Release 8.7 R1; support for IPV4 added. hmac-sha256, hmac-sha384 and hmac-sha512 algorithm added.
**Related Commands**

**show ipsec sa** Displays information about manually configured IPsec Security Associations.

**MIB Objects**

AlaIPsecSAConfigTable
  - AlaIPsecSAConfigName
  - AlaIPsecSAConfigType
  - AlaIPsecSAConfigSource
  - AlaIPsecSAConfigSourceType
  - AlaIPsecSAConfigDestination
  - AlaIPsecSAConfigDestinationType
  - AlaIPsecSAConfigSPI
  - AlaIPsecSAConfigEncryptionAlgorithm
  - AlaIPsecSAConfigEncryptionKeyLength
  - AlaIPsecSAConfigAuthenticationAlgorithm
  - AlaIPsecSAConfigDescription
  - AlaIPsecSAConfigAdminState
ipsec default-discard

Enable or disable the default discard policy.

```
ipsec default-discard {ipv4 | ipv6} admin-state {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the default discard policy.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the default discard policy.</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The default discard policy drops all the inbound traffic that does not match an IPsec policy.
- When incoming traffic is dropped due to the default discard policy, an SWLog informational message is logged.
- The default discard policy on its own drops all the incoming traffic destined for the switch. It is required to add appropriate higher priority policies to allow the desired traffic to be accepted. At a minimum, policies must be added to allow neighbor discovery traffic to be accepted. For example:

  ```
  -> ipsec policy ns-in priority 100 source ::/0 destination ::/0 protocol ICMP6 type 135 in none
  -> ipsec policy na-in priority 100 source ::/0 destination ::/0 protocol ICMP6 type 136 in none
  ```
- The default discard policy will be given the name `default-discard-v6` for IPv6 traffic and `default-discard-v4` for IPv4 traffic when it is enabled. If the name conflicts with an existing user-defined policy, a numeric value will be appended to make the policy name unique (`default-discard-v61` for IPv6 and `default-discard-v41` for IPv4).
- If there is an existing user-defined policy that matches the default discard policy selectors (like source, destination, protocol, direction), then the default-discard policy cannot be enabled.
- The default discard policy is not applied to the forwarded traffic.
**Examples**

-> ipsec default-discard ipv6 admin-state enable
-> ipsec default-discard ipv4 admin-state disable

**Release History**

Release 8.4.1; command introduced.
Release 8.7 R1; IPv4 support added.

**Related Commands**

- **show ipsec policy**
  Displays information about the security policies.

**MIB Objects**

- a1aIPsecConfig
**show ipsec policy**

Displays information about the security policies.

```
show ipsec policy [name | ipv4 | ipv6]
```

**Syntax Definitions**

- **name**
  - The policy name to be specified to request detailed information about an individual policy.

- **ipv4 | ipv6**
  - Displays policy information based on the address type.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *name* parameter to display information about a specific security policy.
- The policy information can also be viewed based on the address type.

**Examples**

```
-> show ipsec policy
IPV4 Default discard policy = Disabled

IPV6 Default discard policy = Enabled
```

```
Name Priority Source->Destination Protocol Direction Action State
-----------------------------------------------+----------+---------+-------------+------
default-discard 1000 ::/0 -> ::/0 any in discard active
ftp-in-drop 100 ::/0->2001:db8:3:13d TCP in discard active
telnet-in-1 100 2001:db8::/48->2001:db8:1::24 TCP in ipsec active
telnet-out-1 100 2001:db8:1::24->2001:db8::/48 TCP out ipsec active
```

```
-> show ipsec policy ipv4
Default ipv4 discard policy = Disabled
```

```
Name Priority Source->Destination Protocol Direction Action State
-----------------------------------------------+----------+---------+-------------+------
udp_in 100 10.1.1.2->10.1.1.1 UDP in ipsec ah active
udp_out 100 10.1.1.1->10.1.1.2 UDP out ipsec ah active
```
-> show ipsec policy ipv6
Default ipv6 discard policy = Disabled

<table>
<thead>
<tr>
<th>Name</th>
<th>Priority</th>
<th>Source -&gt; Destination</th>
<th>Protocol</th>
<th>Direction</th>
<th>Action</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp_in</td>
<td>100</td>
<td>3ffe::200 -&gt; 3ffe::100</td>
<td>TCP</td>
<td>in</td>
<td>ipsec esp</td>
<td>active</td>
</tr>
<tr>
<td>tcp_out</td>
<td>100</td>
<td>3ffe::100 -&gt; 3ffe::200</td>
<td>TCP</td>
<td>out</td>
<td>ipsec esp</td>
<td>active</td>
</tr>
</tbody>
</table>

**output definitions**

**Default discard policy**
Indicates whether the default discard policy is enabled or disabled.

**Name**
The name of the security policy.

**Priority**
The priority set for the policy.

**Source -> Destination**
Indicates the source and destination of traffic covered by this policy.

**Protocol**
Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) is displayed in this field.

**Direction**
Indicates whether the policy has been applied to the incoming or outgoing traffic.

**Action**
Indicates the action to be taken on the traffic covered by this policy.

**State**
Indicates the operational state of this policy.

-> show ipsec policy telnet-out-1
Policy
Name      = telnet-out-1,
Priority  = 100,
Source    = 3ffe:49:49::/48(23),
Destination = 3ffe:123:983::/48,
Protocol  = TCP,
Direction = out,
Action    = ipsec,
State     = active

Rules
1 : esp,
2 : ah

Description
Require AH and ESP headers on outgoing telnet traffic.

**output definitions**

**Name**
The name of the security policy.

**Priority**
The priority set for the policy.

**Source**
Indicates the source of the traffic covered by this policy.

**Destination**
Indicates the destination of the traffic covered by this policy.

**Protocol**
Indicates the protocol traffic covered by this policy. The protocol name (TCP) or protocol number (80) is displayed in this field.

**Direction**
Indicates whether the policy has been applied to the incoming or outgoing traffic.

**Action**
Indicates the action to be taken on the traffic covered by this policy.

**State**
Indicates the operational state of this policy.

**Rules**
The rules specified for the policy.

**Description**
The description of the policy.
**Release History**

Release 7.1.1; command introduced.
Release 8.4.1; **default discard policy** field added.
Release 8.7 R1; **ipv4** and **ipv6** options added.

**Related Commands**

- `ipsec policy` Adds, modifies, or removes a security policy.
- `ipsec default-discard` Enable or disable the default discard policy.

**MIB Objects**

```
AlaIPsecSecurityPolicyTable
   alaIPsecSecurityPolicyName
   alaIPsecSecurityPolicySource
   alaIPsecSecurityPolicySourceType
   alaIPsecSecurityPolicySourcePrefixLength
   alaIPsecSecurityPolicySourcePort
   alaIPsecSecurityPolicyDestination
   alaIPsecSecurityPolicyDestinationType
   alaIPsecSecurityPolicyDestinationPrefixLength
   alaIPsecSecurityPolicyDestinationPort
   alaIPsecSecurityPolicyProtocol
   alaIPsecSecurityPolicyDirection
   alaIPsecSecurityPolicyAction
   alaIPsecSecurityPolicyOperationalState
   alaIPsecSecurityPolicyRuleIndex
   alaIPsecSecurityPolicyRuleProtocol
   alaIPsecSecurityPolicyDescription
```
**show ipsec sa**

Displays information about manually configured IPsec Security Associations.

```
show ipsec sa [name | esp | ah | ipv4 | ipv6]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the Security Association.</td>
</tr>
<tr>
<td>esp</td>
<td>Restricts the display to ESP type SAs.</td>
</tr>
<tr>
<td>ah</td>
<td>Restricts the display to AH type SAs.</td>
</tr>
<tr>
<td>ipv4</td>
<td>ipv6</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `name` parameter to display the information about a specific SA.
- Use `esp` or `ah` option to display the information about their respective type SAs.

### Examples

```
-> show ipsec sa
Name            Type  Source-> Destination [SPI]           State   Encryption      Authentication
-----------------------------------------------------------------------------------------------
telnet-in-esp   ESP  2001:db8::/49->2001:db8:1::24   active   aes-cbc(128)  hmac-sha1
        hmac-shal
        telnet-out-esp ESP 2001:db8:1::24->2001:db8::/48 active   aes-cbc(128)  hmac-sha1
        hmac-shal

-> show ipsec sa ipv6
Name            Type  Source -> Destination [SPI]           Encryption Authentication State
-----------------------------------------------------------------------------------------------
tcp_in_esp1     esp    3ffe::200 -> 3ffe::100 [1000]  null   hmac-shal     active
        tcp_out_esp1 esp    3ffe::100 -> 3ffe::200 [1001]  null   hmac-shal     active
```
-> show ipsec sa ipv4
Name | Type | Source -> Destination [SPI] | Encryption | Authentication | State
-----+------+-----------------------------+------------+---------------+------
udp_in_ah | ah | 10.1.1.2 -> 10.1.1.1 [1002] | null | hmac-sha1 | active
udp_out_ah | ah | 10.1.1.1 -> 10.1.1.2 [1003] | null | hmac-sha1 | active

output definitions

Name | The SA name.
Type | The SA type: AH or ESP.
Source -> Destination [SPI] | The traffic source, traffic destination, and SPI for this SA.
State | The operational state of this SA.
Encryption | The encryption algorithm used for this SA.
Authentication | The authentication algorithm in use for this SA.

-> show ipsec sa telnet-in-esp
Name = telnet-in-esp
Type = ESP
Source = 2001:db8::/48
Destination = 2001:db8:1::24
SPI = 8920
Encryption = aes-cbc(128)
Authentication = hmac-shal
State = active
Description:

output definitions

Name | The SA name.
Type | The SA type: AH or ESP.
Source | The traffic source for this SA.
Destination | The traffic destination for this SA.
SPI | The SA's SPI.
Encryption | The encryption algorithm used for this SA.
Authentication | The authentication algorithm used for this SA.
State | The operational state of this SA.
Description | The SA's description.

Release History
Release 7.1.1; command introduced.
Release 8.7 R1: ipv4 and ipv6 options added.
**Related Commands**

**ipsec sa**

Adds, modifies, or deletes a manually configured IPsec Security Association (SA).

**MIB Objects**

 AlaIPsecSAConfigTable
  - AlaIPsecSAConfigName
  - AlaIPsecSAConfigType
  - AlaIPsecSAConfigSource
  - AlaIPsecSAConfigSourceType
  - AlaIPsecSAConfigDestination
  - AlaIPsecSAConfigDestinationType
  - AlaIPsecSAConfigSPI
  - AlaIPsecSAConfigOperationalState
  - AlaIPsecSAConfigEncryptionAlgorithm
  - AlaIPsecSAConfigEncryptionKeyLength
  - AlaIPsecSAConfigAuthenticationAlgorithm
  - AlaIPsecSAConfigAuthenticationKeyLength
  - AlaIPsecSAConfigDescription
**show ipsec key**

Displays the keys for the manually configured IPsec SA.

`show ipsec key [sa-encryption | sa-authentication]`

---

### Syntax Definitions

- **sa-encryption**: Displays the encryption keys.
- **sa-authentication**: Displays the authentication keys.

---

### Defaults

N/A

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

The key values are not be displayed due to security reasons.

---

### Examples

```
-> show ipsec key sa-encryption
Encryption Keys
Name                 Length (bits)
--------------------+-------------
sa_1                192
sa_2                160
sa_3                 64

-> show ipsec key sa-authentication
Authentication Keys
Name                 Length (bits)
--------------------+-------------
sa_1                128
sa_5                 160
```

---

### output definitions

- **Name**: The name of the SA for which the key is used.
- **Length**: The length of the key in bits.
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**ipsec key**  
Adds, modifies or deletes the authentication and encryption keys for a manually configured IPsec SA.

**MIB Objects**

AlaIPsecKeyTable
   alaIPsecKeyName
   alaIPsecKey
**show ipsec statistics**

Displays IPsec statistics.

**show ipsec statistics**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> show ipsec statistics`

Inbound:
- Discarded = 0,
- No SA found = 0,
- Policy violation = 0,
- Authentication failure = 0,
- Replay check failed = 0,
- Other error = 0

Outbound:
- Discarded = 0,
- No SA found = 0,
- Other error = 0

**output definitions**

- **Discarded (Inbound)**: The number of incoming packets discarded because they matched a discard policy.
- **No SA found (Inbound)**: The number of incoming packets dropped because of no matching SA found.
### output definitions

<table>
<thead>
<tr>
<th>Policy violation (Inbound)</th>
<th>The number of incoming packets that don’t have the IPsec protection required by a security policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Failure (Inbound)</td>
<td>The number of incoming packets that failed authentication.</td>
</tr>
<tr>
<td>Replay check failed (Inbound)</td>
<td>The number of incoming packets that failed a replay check.</td>
</tr>
<tr>
<td>Other error (Inbound)</td>
<td>The number of incoming packets dropped for a reason not otherwise counted.</td>
</tr>
<tr>
<td>Discarded (Outbound)</td>
<td>The number of outgoing packets discarded because they matched a discard policy.</td>
</tr>
<tr>
<td>No SA found (Outbound)</td>
<td>The number of outgoing packets dropped because of no matching SA found.</td>
</tr>
<tr>
<td>Other error (Outbound)</td>
<td>The number of outgoing packets dropped for a reason not otherwise counted.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command introduced.
Release 8.7 R1; Support for IPV4 added.

### Related Commands

- `show ipsec policy` Displays information about the security policies.
- `show ipsec sa` Displays information about manually configured IPsec Security Associations.

### MIB Objects

- `AlaIPsecStatisticsTable`
  - `alaIPsecStatisticsInDiscarded`
  - `alaIPsecStatisticsInPolicyViolation`
  - `alaIPsecStatisticsInAHAuthenticationFail`
  - `alaIPsecStatisticsInNoSA`
  - `alaIPsecErrorsInReplay`
  - `alaIPsecErrorsInOther`
  - `alaIPsecStatisticsOutDiscarded`
  - `alaIPsecStatisticsOutPolicyViolation`
  - `alaIPsecErrorsOutOther`
  - `alaIPsecStatisticsOutNoSA`
Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) that uses hop count as its routing metric. RIP-enabled switches update neighboring switches by transmitting a copy of their own routing table. The RIP routing table always uses the most efficient route to a destination, that is, the route with the fewest hops and longest matching prefix.

The switch supports RIP version 1 (RIPv1), RIP version 2 (RIPv2), and RIP next generation (RIPng). It also supports simple and MD5 authentication, on an interface basis, for RIPv2.

The RIP commands comply with the following RFCs: RFC1058, RFC2453, RFC1722, RFC1723, RFC1724, and RFC2080.

MIB information for the RIP commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-VIRTUALROUTER-MIB.mib</td>
<td>alcatelIND1VirtualRouterMIB</td>
</tr>
<tr>
<td>RIPv2-MIB.mib</td>
<td>rip2</td>
</tr>
<tr>
<td>ALCATEL-IND1-ripng-MIB.mib</td>
<td>alcatelIND1RipngMIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>IP Command</th>
<th>IPv6 Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip load rip</td>
<td>ipv6 load rip</td>
</tr>
<tr>
<td>ip rip admin-state</td>
<td>ipv6 rip admin-state</td>
</tr>
<tr>
<td>ip rip interface</td>
<td>ipv6 rip invalid-timer</td>
</tr>
<tr>
<td>ip rip interface admin-state</td>
<td>ipv6 rip garbage-timer</td>
</tr>
<tr>
<td>ip rip interface metric</td>
<td>ipv6 rip holddown-timer</td>
</tr>
<tr>
<td>ip rip interface send-version</td>
<td>ipv6 rip jitter</td>
</tr>
<tr>
<td>ip rip interface recv-version</td>
<td>ipv6 rip route-tag</td>
</tr>
<tr>
<td>ip rip interface ingress-filter</td>
<td>ipv6 rip update-interval</td>
</tr>
<tr>
<td>ip rip interface egress-filter</td>
<td>ipv6 rip triggered-sends</td>
</tr>
<tr>
<td>ip rip force-holddowntimer</td>
<td>ipv6 rip interface</td>
</tr>
<tr>
<td>ip rip host-route</td>
<td>ipv6 rip interface metric</td>
</tr>
<tr>
<td>ip rip route-tag</td>
<td>ipv6 rip interface recv-status</td>
</tr>
<tr>
<td>ip rip interface auth-type</td>
<td>ipv6 rip interface send-status</td>
</tr>
<tr>
<td>ip rip interface auth-key</td>
<td>ipv6 rip interface horizon</td>
</tr>
<tr>
<td>ip rip update-interval</td>
<td>show ipv6 rip</td>
</tr>
<tr>
<td>ip rip invalid-timer</td>
<td>show ipv6 rip interface</td>
</tr>
<tr>
<td>ip rip holddown-timer</td>
<td>show ipv6 rip peer</td>
</tr>
<tr>
<td>show ip rip</td>
<td>show ipv6 rip routes</td>
</tr>
<tr>
<td>show ip rip routes</td>
<td></td>
</tr>
<tr>
<td>show ip rip interface</td>
<td></td>
</tr>
<tr>
<td>show ip rip peer</td>
<td></td>
</tr>
</tbody>
</table>
**ip load rip**

Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.

`ip load rip`

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- In simple networks where only IP forwarding is required, you may not want to use RIP. If you are not using RIP, it is best not to load it to save switch resources.

- To remove RIP from switch memory, you must manually edit the `boot.cfg` file. The `boot.cfg` file is an ASCII text-based file that controls many of the switch parameters. Open the file and delete all references to RIP. You must reboot the switch when this is complete.

- Use the `ip rip admin-state` command to enable RIP on the switch.

**Examples**

`-> ip load rip`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip rip admin-state**: Enables/disables RIP routing on the switch.
- **show ip rip**: Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

MIB Objects

- **alaVrConfigTable**
  - **alaVrConfigRipStatus**
ip rip admin-state

Enables/disables RIP on the switch. RIP performs well in small networks. By default, RIP packets are broadcast every 30 seconds, even if no change has occurred anywhere in a route or service. Depending on the size and speed of the network, these periodic broadcasts can consume a significant amount of bandwidth.

ip rip admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables RIP routing on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables RIP routing on the switch.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- RIP must be loaded on the switch (ip load rip) to enable RIP on the switch.
- A RIP network can be no more than 15 hops (end-to-end). If there is a 16th hop, that network is identified as infinity and the packet is discarded.

Examples

- ip rip admin-state enable

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **ip load rip**
  Loads RIP into the switch memory.

- **show ip rip**
  Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

**MIB Objects**

- **alaProtocolRip**
- **alaRipProtoStatus**
**ip rip interface**

Creates/deletes a RIP interface. Routing is enabled on a VLAN when you create a router interface. However, to enable RIP routing, you must also configure and enable a RIP routing interface on the VLAN’s IP router interface.

**ip rip interface**  
```
{interface_name}
```

**no ip rip interface**  
```
{interface_name}
```

### Syntax Definitions

**interface_name**  
The name of the interface.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- By default, a RIP interface is created in the disabled state. To enable RIP routing on the interface, you must enable the interface by using the **ip rip interface admin-state** command.

- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.

- For more information on VLANs and router ports, see Chapter 5, “VLAN Management Commands”.

### Examples

```
-> ip rip interface rip-1
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

**ip interface**
Creates a VLAN router interface.

**ip load rip**
Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.

**ip rip admin-state**
Enables/disables RIP routing on the switch.

**ip rip interface admin-state**
Enables/disables a RIP interface.

**MIB Objects**

rip2IfConfTable
  rip2IfConfAddress
  rip2IfConfStatus
ip rip interface admin-state

Enables and disables a RIP interface. By default, a RIP interface is created in the disabled state. After creating a RIP interface, you must use this command to enable the interface.

`ip rip interface {interface_name} admin-state {enable | disable}`

**Syntax Definitions**

- `interface_name`: The name of the interface.
- `enable`: Administratively enables RIP on the interface.
- `disable`: Administratively disables RIP on the interface.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- You must first create a RIP interface by using the `ip rip interface` command before enabling the interface.
- You can create a RIP interface even if an IP router interface has not been configured. However, RIP will not function unless an IP router interface is configured with the RIP interface.
- For more information on VLANs and router ports, see Chapter 5, “VLAN Management Commands”.

**Examples**

`-> ip rip interface rip-1 admin-state enable`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip interface` Creates a VLAN router interface.
- `ip load rip` Loads RIP into memory. When the switch is initially configured, you must load RIP into memory before it can be enabled.
- `ip rip admin-state` Enables/disables RIP routing on the switch.
- `ip rip interface` Creates/deletes a RIP interface.

**MIB Objects**

- `rip2IfConfTable`
- `rip2IfConfAddress`
- `rip2IfConfStatus`
**ip rip interface metric**

Configures the RIP metric or cost for a specified interface. You can set priorities for routes generated by a switch by assigning a metric value to routes generated by that switch’s RIP interface. For example, routes generated by a neighboring switch may have a hop count of 1. However, you can lower the priority of routes generated by that switch by increasing the metric value for routes generated by the RIP interface.

```
ip rip interface {interface_name} metric value
```

### Syntax Definitions

- **interface_name**
  - The name of the interface.

- **value**
  - Metric value. Valid range is 1–15.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570N</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When you configure a metric for a RIP interface, this metric cost is added to the metric of the incoming route.

### Examples

```
-> ip rip interface rip-1 metric 2
```

### Release History

Release 7.1.1; command was introduced.


**Related Commands**

- **ip rip interface**  
  Enables/disables RIP on a specific interface.

- **show ip rip peer**  
  Displays active RIP neighbors (peers). An active peer is a switch that has sent a RIP packet within the last 180 seconds.

**MIB Objects**

- **rip2IfConfTable**
  - **rip2IfConfAddress**
  - **rip2IfConfDefaultMetric**
ip rip interface send-version

Configures the send option for a RIP interface. This defines the type(s) of RIP packets that the interface will send.

ipa rip interface \{interface_name\} send-version \{none | v1 | v1compatible | v2\}

**Syntax Definitions**

<table>
<thead>
<tr>
<th>interface_name</th>
<th>The name of the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>RIP packets will not be sent by the interface.</td>
</tr>
<tr>
<td>v1</td>
<td>Only RIPv1 packets will be sent by the interface.</td>
</tr>
<tr>
<td>v1compatible</td>
<td>Only RIPv2 broadcast packets (not multicast) will be sent by the interface.</td>
</tr>
<tr>
<td>v2</td>
<td>Only RIPv2 packets will be sent by the interface.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>v1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Using this command will override RIP default behavior.
- Other devices must be able to interpret the information provided by this command or there will not be proper routing information exchanged between the switch and other devices on the network.

**Examples**

```bash
-> ip rip interface rip-1 send-version v1
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

`ip rip interface recv-version` Configures the receive option for a RIP interface.

MIB Objects

`rip2IfConfTable`
  `rip2IfConfAddress`
  `rip2IfConfSend`
ip rip interface recv-version

Configures the receive option for a RIP interface. This defines the type(s) of RIP packets that the interface will accept.

```
ip rip interface {interface_name} recv-version {v1 | v2 | both | none}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>interface_name</th>
<th>The name of the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>Only RIPv1 packets will be received by the interface.</td>
</tr>
<tr>
<td>v2</td>
<td>Only RIPv2 packets will be received by the interface.</td>
</tr>
<tr>
<td>both</td>
<td>Both RIPv1 and RIPv2 packets will be received by the interface.</td>
</tr>
<tr>
<td>none</td>
<td>Interface ignores any RIP packets received.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td>v2</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Using this command will override RIP default behavior.
- Other devices must be able to interpret the information provided by this command or there will not be proper routing information exchanged between the switch and other devices on the network.

### Examples

```
-> ip rip interface rip-1 recv-version both
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ip rip interface send-version` Configures the send option for a RIP interface.

**MIB Objects**

- `rip2IfConfTable`
  - `rip2IfConfAddress`
  - `rip2IfConfReceive`
ip rip interface ingress-filter

Assigns an ingress route map filter to the specified RIP interface. Received route advertisements are compared against ingress filters. When a prefix matches the corresponding filter, that prefix is accepted on the interface. When a prefix does not match the filter, the prefix is dropped as if it was never received.

**Syntax Definitions**

interface_name
The name of an existing RIP interface.

filter_name
The name of an existing route-map filter.

**Defaults**

By default, no such filter is associated with the RIP interface.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- One route-map filter is configurable in each direction (ingress/egress) for each RIP interface.
- Configuring multiple filters in the same direction for a single RIP interface is not supported.

**Examples**

```
-> ip route-map ripfilter1 action permit
-> ip route-map ripfilter1 match ip-address 202.5.0.0/16 deny
-> ip rip interface vlan-100 Ingress-filter RipFilter1
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ip rip interface egress-filter** Assigns an egress route map filter to a RIP interface.
- **show ip rip interface** Displays RIP interface status and configuration.

**MIB Objects**

- N/A
ip rip interface egress-filter

Assigns an egress route map filter to the specified RIP interface. Outbound route advertisements are compared against egress filters. When a prefix matches the corresponding filter, that prefix is sent on the interface. When a prefix does not match the filter, the prefix is dropped as if it did not exist in the RIP RIB.

**ip rip interface {interface_name} egress-filter {filter_name}**

### Syntax Definitions

- **interface_name**: The name of an existing RIP interface.
- **filter_name**: The name of an existing route-map filter.

### Defaults

By default, no such filter is associated with the RIP interface.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- One route-map filter is configurable in each direction (ingress/egress) for each RIP interface.
- Configuring multiple filters in the same direction for a single RIP interface is not supported.

### Examples

- ip route-map ripfilter1 action permit
- ip route-map ripfilter1 match ip-address 202.5.0.0/16 deny
- ip rip interface vlan-100 egress-filter RipFilter1

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip rip interface egress-filter**: Assigns an ingress route map filter to a RIP interface.
- **show ip rip interface**: Displays RIP interface status and configuration.

MIB Objects

- **N/A**
ip rip force-holddowntimer

Configures the forced hold-down timer value, in seconds, that defines an amount of time during which routing information regarding better paths is suppressed. A route enters into a forced hold-down state when an update packet is received that indicates the route is unreachable and when this timer is set to a non-zero value. After this timer has expired and if the value is less than 120 seconds, the route enters a hold-down state for the rest of the period until the remainder of the 120 seconds has also expired. During this time the switch will accept any advertisements for better paths that are received.

**ip rip force-holddowntimer seconds**

### Syntax Definitions

- **seconds**: The forced hold-down time interval. The valid range is 0–120 seconds.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The forced hold-down timer is not the same as the RIP hold-down timer. The forced hold-down timer defines a separate interval that overlaps the hold-down state. During the forced hold-down timer interval, the switch will not accept better routes from other gateways.

- The forced hold-down time interval can become a subset of the hold-down timer (120 seconds) by using this command to set a value less than 120.

- To allow the routing switch to use better routes advertised during the entire hold-down time period, leave the forced hold-down timer set to the default value.

### Examples

```
-> ip rip force-holddowntimer 10
```

### Release History

Release 7.1.1; command was introduced.
RIP Commands

ip rip force-holddowntimer

Related Commands

show ip rip
Displays the RIP status and general configuration parameters (for example, forced hold-down timer).

MIB Objects

alaProtocolRip
alaRipForceHolddownTimer
**ip rip host-route**

Specifies whether or not RIP can add host routes (routes with a 32-bit mask) to the RIP table.

**ip rip host-route**

**no ip rip host-route**

---

**Syntax Definitions**

N/A

**Defaults**

The default is to enable a default host route.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to prevent RIP from adding host routes to the RIP table.
- When enabled, RIPv1 will interpret an incoming route announcement that contains any 1 bit in the host portion of the IP address as a host route, implying a mask of 255.255.255.255.

**Examples**

-> ip rip host-route

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip rip routes` Displays the RIP Routing Database.

**MIB Objects**

alaProtocolRip
alaRipHostRouteSupport
**ip rip route-tag**

Configures the route tag value for RIP routes generated by the switch.

`ip rip route-tag value`

---

**Syntax Definitions**

`value`  
Route tag value. Valid range is 0–2147483647.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Only RIPv2 supports route tags.

**Examples**

`-> ip rip route-tag 0`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip rip`  
  Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

**MIB Objects**

- `alaRipRedistRouteTag`
ip rip interface auth-type

Configures the type of authentication that will be used for the RIP interface. By default, there is no authentication used for RIP. However, you can configure a password for a RIP interface. To configure a password, you must first select the authentication type (simple or MD5), then configure a password.

ip rip interface {interface_name} auth-type {none | simple | md5}

Syntax Definitions

- **interface_name**: The name of the interface.
- **none**: No authentication will be used.
- **simple**: Simple authentication will be used.
- **md5**: MD5 authentication will be used.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>simple</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platforms Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

Regardless of which authentication type is used (simple or MD5), both switches on either end of a link must share the same password.

Examples

- `-> ip rip interface rip-1 auth-type none`

Release History

Release 7.1.1; command was introduced.
Related Commands

ip rip interface auth-key  Configures the text string that will be used as the password for the RIP interface.

MIB Objects

rip2IfConfTable
   rip2IfConfAddress
   rip2IfConfAuthType
ip rip interface auth-key

Configures the text string that will be used as the password for the RIP interface. If you configure simple or MD5 authentication, you must configure a text string that will be used as the password for the RIP interface.

ip rip interface {interface_name} auth-key string

Syntax Definitions

interface_name
The name of the interface.

string
16-byte text string.

Defaults

The default authentication string is a null string.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Regardless of which authentication type is used (simple or MD5), both switches on either end of a link must share the same password.

Examples

-> ip rip interface rip-1 auth-key nms

Release History

Release 7.1.1; command was introduced.
Related Commands

`ip rip interface auth-type`  
Configures the type of authentication that will be used for the RIP interface.

**MIB Objects**

- `rip2IfConfTable`
- `rip2IfConfAddress`
- `rip2IfConfAuthKey`
ip rip update-interval

Configures the time interval during which RIP routing updates are sent out.

`ip rip update-interval seconds`

**Syntax Definitions**

`seconds` The RIP routing update interval, in seconds. The valid range is 1–120.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The update interval value must be less than or equal to one-third the invalid interval value.

**Examples**

```
-> ip rip update-interval 45
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip rip` Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

**MIB Objects**

- `alaProtocolRip`  
  - `alaRipUpdateInterval`
**ip rip invalid-timer**

Configures the RIP invalid timer value that defines the time interval during which a route will remain active in Routing Information Base (RIB) before moving to the invalid state.

**ip rip invalid-timer seconds**

---

**Syntax Definition**

*seconds*  
The RIP invalid timer value, in seconds. The valid range is 3–360.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>180</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The invalid time interval value must be three times the update interval value.

**Examples**

-> ip rip invalid-timer 270

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**show ip rip**  
Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

**MIB Objects**

alaProtocolRip  
alaRipInvalidTimer
**ip rip garbage-timer**

Configures the RIP garbage timer value that defines the time interval, which must elapse before an expired route is removed from the RIB.

**ip rip garbage-timer seconds**

---

**Syntax Definition**

*seconds*  
The RIP garbage timer value, in seconds. The valid range is 0–180.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>seconds</em></td>
<td>120</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

|        | 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 V72/C32 | 6900 X48C6/T48C6/  
|--------|------|------|------|-------|------|-------|------|------|------------ | X48C4E/V48C8/  
| No     | Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes          | C32E/T24C2/   
|        |      |      |      |       |      |       |      |      | X24C2       |        |

**Usage Guidelines**

During the RIP garbage interval, the router advertises the route with a metric of INFINITY (i.e., 16 hops).

**Examples**

`-> ip rip garbage-timer 180`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

*show ip rip*  
Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

**MIB Objects**

*alaProtocolRip*  
*alaRipGarbageTimer*
**ip rip holddown-timer**

Configures the RIP hold-down timer value that defines the time interval during which a route remains in the hold-down state.

`ip rip holddown-timer seconds`

### Syntax Definition

`seconds` The hold-down time interval, in seconds. The valid range is 0–120.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When RIP detects a route with higher metric than the route in the RIB, the route with the higher metric goes into the hold-down state. The route updates with a metric of INFINITY are rejected.

### Examples

-> ip rip holddown-timer 10

### Release History

Release 7.1.1; command was introduced.

### Related Commands

**show ip rip** Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

### MIB Objects

alaProtocolRip
alaRipHolddownTimer
**show ip rip**

Displays the RIP status and general configuration parameters (e.g., forced hold-down timer).

```plaintext
-> show ip rip
```

<table>
<thead>
<tr>
<th>Syntax Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platforms Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command is supported on the following OmniSwitch platforms:</td>
</tr>
<tr>
<td>No Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>-&gt; show ip rip</td>
</tr>
</tbody>
</table>

Status = Enabled
Number of routes = 9
Host Route Support = Enabled
Route Tag = 42
Update interval = 30
Invalid interval = 180
Garbage interval = 120
Holddown interval = 0
Forced Hold-Down Timer = 0

<table>
<thead>
<tr>
<th>output definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Number of routes</td>
</tr>
<tr>
<td>Host Route Support</td>
</tr>
<tr>
<td>Route Tag</td>
</tr>
<tr>
<td>Update interval</td>
</tr>
</tbody>
</table>
**RIP Commands**

```
show ip rip
```

### Output Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Invalid interval</strong></td>
<td>The RIP invalid timer value, in seconds.</td>
</tr>
<tr>
<td><strong>Garbage interval</strong></td>
<td>The RIP garbage timer value, in seconds.</td>
</tr>
<tr>
<td><strong>Holddown interval</strong></td>
<td>The hold-down time interval, in seconds.</td>
</tr>
<tr>
<td><strong>Forced Hold-Down Timer</strong></td>
<td>The forced hold-down time interval, in seconds.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **ip rip admin-state** Enables/disables RIP routing on the switch.
- **ip rip force-holddowntimer** Configures the interval during which a RIP route remains in the forced hold-down state.
- **ip rip update-interval** Configures the time interval during which RIP routing updates are sent out.
- **ip rip invalid-timer** Configures the RIP invalid timer value that defines the time interval during which a route will remain active in Routing Information Base (RIB) before moving to the invalid state.
- **ip rip garbage-timer** Configures the RIP garbage timer value that defines the time interval, which must elapse before an expired route is removed from the RIB.
- **ip rip holddown-timer** Configures the RIP hold-down timer value that defines the time interval during which a route remains in the hold down state.

### MIB Objects

- **alaProtocolRip**
  - **alaRipProtoStatus**
  - **alaRipRouteNumber**
  - **alaRipHostRouteSupport**
  - **alaRipRedistRouteTag**
  - **alaRipUpdateInterval**
  - **alaRipInvalidTimer**
  - **alaRipGarbageTimer**
  - **alaRipHolddownTimer**
  - **alaRipForceHolddownTimer**
show ip rip routes

Displays the RIP routing database. The routing database contains all of the routes learned through RIP.

\texttt{show ip rip routes [ip\_address ip\_mask]}

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{ip_address}</td>
<td>32-bit IP address.</td>
</tr>
<tr>
<td>\texttt{ip_mask}</td>
<td>The mask corresponding to the IP address.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view all RIP routes, enter the basic command syntax (\texttt{show ip rip routes}). To view a specific route, enter the destination IP address and mask.

**Examples**

-> show ip rip routes

Legends: State: A = Active, H = Holddown, G = Garbage

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>State</th>
<th>Metric</th>
<th>Proto</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0.0.0/8</td>
<td>+5.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>4.0.0.7</td>
<td>A</td>
<td>3</td>
<td>Rip</td>
</tr>
<tr>
<td>4.0.0.0/8</td>
<td>+5.0.0.14</td>
<td>A</td>
<td>3</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>2.0.0.14</td>
<td>A</td>
<td>3</td>
<td>Rip</td>
</tr>
<tr>
<td>5.0.0.0/8</td>
<td>+2.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>4.0.0.7</td>
<td>A</td>
<td>3</td>
<td>Rip</td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>+4.0.0.7</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>5.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>2.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>+5.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>2.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>4.0.0.7</td>
<td>A</td>
<td>3</td>
<td>Rip</td>
</tr>
<tr>
<td>128.251.40.0/24</td>
<td>+4.0.0.7</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>5.0.0.14</td>
<td>A</td>
<td>3</td>
<td>Rip</td>
</tr>
<tr>
<td></td>
<td>2.0.0.14</td>
<td>A</td>
<td>3</td>
<td>Rip</td>
</tr>
</tbody>
</table>
### show ip rip routes

<table>
<thead>
<tr>
<th>Destination Network</th>
<th>Gateway</th>
<th>Metric</th>
<th>State</th>
<th>Age</th>
<th>Tag</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>150.0.0.0/24</td>
<td>+4.0.0.7</td>
<td>A</td>
<td>2</td>
<td>19s</td>
<td>0</td>
<td>Rip</td>
</tr>
<tr>
<td>5.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Active</td>
<td>19s</td>
<td>0</td>
<td>Rip</td>
</tr>
<tr>
<td>2.0.0.14</td>
<td>A</td>
<td>2</td>
<td>Active</td>
<td>12s</td>
<td>0</td>
<td>Rip</td>
</tr>
<tr>
<td>152.0.0.0/24</td>
<td>+4.0.0.7</td>
<td>A</td>
<td>2</td>
<td>19s</td>
<td>0</td>
<td>Rip</td>
</tr>
<tr>
<td>5.0.0.14</td>
<td>A</td>
<td>3</td>
<td>Active</td>
<td>12s</td>
<td>0</td>
<td>Rip</td>
</tr>
</tbody>
</table>

#### output definitions

<table>
<thead>
<tr>
<th>Destination</th>
<th>Destination network IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>The Gateway IP address (switch from which the destination address was learned).</td>
</tr>
<tr>
<td>State</td>
<td>The associated state of the route, which can be A (Active), H (Holddown), or G (Garbage).</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric associated with this network. Generally, this is the RIP hop count (the number of hops from this switch to the destination switch).</td>
</tr>
<tr>
<td>Proto</td>
<td>The type of route (Local, Rip, or Redist).</td>
</tr>
</tbody>
</table>

```plaintext
-> show ip rip routes 2.0.0.0 255.0.0.0

<table>
<thead>
<tr>
<th>Destination</th>
<th>2.0.0.0.0,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask length</td>
<td>8,</td>
</tr>
<tr>
<td>Gateway(1)</td>
<td>5.0.0.14,</td>
</tr>
<tr>
<td>Protocol</td>
<td>Rip,</td>
</tr>
<tr>
<td>Out Interface</td>
<td>intf5,</td>
</tr>
<tr>
<td>Metric</td>
<td>2,</td>
</tr>
<tr>
<td>Status</td>
<td>Installed,</td>
</tr>
<tr>
<td>State</td>
<td>Active,</td>
</tr>
<tr>
<td>Age</td>
<td>19s,</td>
</tr>
<tr>
<td>Tag</td>
<td>0,</td>
</tr>
<tr>
<td>Gateway(2)</td>
<td>4.0.0.7,</td>
</tr>
<tr>
<td>Protocol</td>
<td>Rip,</td>
</tr>
<tr>
<td>Out Interface</td>
<td>intf4,</td>
</tr>
<tr>
<td>Metric</td>
<td>3,</td>
</tr>
<tr>
<td>Status</td>
<td>Not Installed,</td>
</tr>
<tr>
<td>State</td>
<td>Active,</td>
</tr>
<tr>
<td>Age</td>
<td>12s,</td>
</tr>
<tr>
<td>Tag</td>
<td>0,</td>
</tr>
</tbody>
</table>
```

#### output definitions

<table>
<thead>
<tr>
<th>Destination</th>
<th>Destination network IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask length</td>
<td>Length of the destination network IP subnet mask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The Gateway IP address (switch from which the destination address was learned).</td>
</tr>
<tr>
<td>Protocol</td>
<td>The type of the route (Local, Rip, or Redist).</td>
</tr>
<tr>
<td>Out Interface</td>
<td>The RIP interface through which the next hop is reached.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric associated with this network. Generally, this is the RIP hop count (the number of hops from this switch to the destination switch).</td>
</tr>
<tr>
<td>Status</td>
<td>The RIP interface status (Installed or Not Installed).</td>
</tr>
<tr>
<td>State</td>
<td>The associated state of the route (Active, Holddown, or Garbage).</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>The age of the route in seconds (the number of seconds since this route was last updated or otherwise determined to be correct).</td>
</tr>
<tr>
<td>Tag</td>
<td>The associated route tag.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

ip rip host-route

Enables/disables a host route to an individual host on a network.

MIB Objects

alaRipEcmpRouteTable
   alaRipEcmpRouteDest
   alaRipEcmpRouteMask
   alaRipEcmpRouteNextHop
   alaRipEcmpRouteType
   alaRipEcmpMetric
   alaRipEcmpStatus
   alaRipEcmpAge
   alaRipEcmpTag
   alaRipEcmpRouteState
   alaRipEcmpRouteStatus
show ip rip interface

Displays RIP interface status and configuration.

**show ip rip interface [interface_name]**

### Syntax Definitions

*interface_name*  
The interface name.

### Defaults

By default, the status and configuration for all RIP interfaces is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Enter an interface name to view detailed information for a specific interface.

### Examples

```bash
-> show ip rip interface
Interface Name Domain Name Domain ID Intf Admin Status IP Intf Status Updates
v12          Vlan    12    disabled    enabled     0/0(0)
s101         Service 101 enabled    enabled     0/0(0)
t1           Tunnel  NA    disabled    disabled    0/0(0)
```

```bash
-> show ip rip interface v12
Interface IP Name = v12,
Interface IP Address = 12.1.1.1,
Domain Name = Vlan,
Domain ID = 12,
Interface Admin status = disabled,
IP Interface Status = enabled,
Interface Config Ingress Route Map Name = ,
Interface Config Egress Route Map Name = ,
Interface Config AuthType = None,
Interface Config AuthKey Length = 0,
Interface Config Send-Version = v2,
Interface Config Receive-Version = both,
Interface Config Default Metric = 1,
Received Packets = 0,
```
show ip rip interface

- Received Bad Packets = 0,
- Received Bad Routes = 0,
- Sent Updates = 0
- show ip rip interface s101
  - Interface IP Name = s101,
  - Interface IP Address = 13.1.1.1,
  - Domain Name = Service,
  - Domain ID = 101,
  - Interface Admin status = enabled,
  - IP Interface Status = enabled,
  - Interface Config Ingress Route Map Name = ,
  - Interface Config Egress Route Map Name = ,
  - Interface Config AuthType = None,
  - Interface Config AuthKey Length = 0,
  - Interface Config Send-Version = v2,
  - Interface Config Receive-Version = both,
  - Interface Config Default Metric = 1,
  - Received Packets = 77564,
  - Received Bad Packets = 0,
  - Received Bad Routes = 0,
  - Sent Updates = 77557

- show ip rip interface t1
  - Interface IP Name = t1,
  - Interface IP Address = 10.1.1.2,
  - Domain Name = Tunnel,
  - Domain ID = NA,
  - Interface Admin status = enabled,
  - IP Interface Status = enabled,
  - Interface Config Ingress Route Map Name = ,
  - Interface Config Egress Route Map Name = ,
  - Interface Config AuthType = None,
  - Interface Config AuthKey Length = 0,
  - Interface Config Send-Version = v2,
  - Interface Config Receive-Version = both,
  - Interface Config Default Metric = 1,
  - Received Packets = 0,
  - Received Bad Packets = 0,
  - Received Bad Routes = 0,
  - Sent Updates = 0

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface IP Name</td>
<td>The IP Interface name.</td>
</tr>
<tr>
<td>Interface IP Address</td>
<td>Interface IP address.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain on which the IP interface was configured (VLAN, Service, or Tunnel).</td>
</tr>
<tr>
<td>Domain ID</td>
<td>The VLAN ID or service ID on which the IP interface was configured. This field displays “NA” for IP tunnels.</td>
</tr>
<tr>
<td>Interface Admin Status</td>
<td>The RIP administrative status (enabled/disabled).</td>
</tr>
<tr>
<td>IP Interface Status</td>
<td>Interface status (enabled /disabled).</td>
</tr>
<tr>
<td>Interface Config Ingress Route Map Name</td>
<td>The name of the route map applied to filter RIP routing updates received on the interface.</td>
</tr>
<tr>
<td>Interface Config Egress Route Map Name</td>
<td>The name of the route map applied to filter RIP routing updates sent on the interface.</td>
</tr>
<tr>
<td>Interface Config AuthType</td>
<td>The type of authentication used for the RIP interface (None or Simple).</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.
Release 8.6R2; “Domain Name” and “Domain ID” fields added.

**Related Commands**

`ip rip interface` Enables/disables RIP for a specific interface.

**MIB Objects**

- `alaProtocolRip`
  - `alaRipProtoStatus`

- `alaRip2IfConfAugTable`
  - `alaRip2IfConfEncryptKey`
  - `alaRip2IfIpConfStatus`
  - `alaRip2IfRec<Pkt>`
  - `alaRip2IfConfName`
  - `alaRip2IfConfType`
  - `alaRip2IfConfPtoPPeer`
  - `alaRip2IfConfIngressFilterRouteMapName`
  - `alaRip2IfConfEgressFilterRouteMapName`
  - `alaRip2IfIfIndex`

- `rip2IfConfTable`
  - `rip2IfConfAddress`
  - `rip2IfConfAuthType`
  - `rip2IfConfAuthKey`
  - `rip2IfConfSend`
  - `rip2IfConfReceive`
  - `rip2IfConfDefaultMetric`

- `rip2IfStatTable`
  - `rip2IfStatRcvBadPackets`
  - `rip2IfStatRcvBadRoutes`
  - `rip2IfStatSentUpdates`
**show ip rip peer**

Displays active RIP neighbors (peers). An active peer is a switch that has sent a RIP packet within the last 180 seconds. If a peer does not send a RIP packet (request or response) within 180 seconds, it is aged out and will not be displayed.

**show ip rip peer [ip_address]**

---

**Syntax Definitions**

*ip_address* 
32-bit IP address.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

```bash
-> show ip rip peer

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Total recvd</th>
<th>Bad Packets</th>
<th>Bad Routes</th>
<th>Version</th>
<th>Secs since last update</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.10.10.1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
```

---

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Peer IP address.</td>
</tr>
<tr>
<td>Total recvd</td>
<td>Total number of RIP packets received from the peer.</td>
</tr>
<tr>
<td>Bad Packets</td>
<td>Number of bad packets received from peer.</td>
</tr>
<tr>
<td>Bad Routes</td>
<td>Number of bad routes received from peer.</td>
</tr>
<tr>
<td>Version</td>
<td>Peer's RIP version as seen on the last packet received.</td>
</tr>
<tr>
<td>Secs since last update</td>
<td>Number of seconds since the last packet was received from the peer.</td>
</tr>
</tbody>
</table>
**Release History**
Release 7.1.1; command was introduced.

**Related Commands**

- `show ip rip interface` Displays the RIP interface status and configuration.

**MIB Objects**

- `rip2PeerTable`
  - `rip2PeerAddress`
  - `rip2PeerDomain`
  - `rip2PeerLastUpdate`
  - `rip2PeerVersion`
  - `rip2PeerRcvBadPackets`
  - `rip2PeerRcvBadRoutes`
ipv6 load rip

Loads RIPng into memory. When the switch is initially configured, you must load RIPng into memory to enable RIPng routing.

ipv6 load rip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- RIPng will support a maximum of 1,000 routes.
- RIPng will support a maximum of 20 interfaces.
- Use the `ipv6 rip admin-state` command to enable RIPng on the switch.

Examples

-> ipv6 load rip

Release History

Release 7.1.1; command was introduced.

Related Commands

- `ipv6 rip admin-state` Enables/disables RIPng routing on the switch.
- `show ipv6 rip` Displays RIPng status and general configuration parameters.

MIB Objects

- `alaDrcTmConfig` `alaDrcTmTIPRipngStatus`
**ipv6 rip admin-state**

Enables or disables RIPng on the switch.

`ipv6 rip admin-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables RIPng.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables RIPng.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

RIPng must be loaded on the switch (**ip load rip**) to enable RIP on the switch.

**Examples**

```
-> ipv6 rip admin-state enable
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip load rip** Loads RIPng into memory.
- **show ipv6 rip** Displays RIPng status and general configuration parameters.

**MIB Objects**

- `alaProtocolripng`
- `alaRipngProtoStatus`
**ipv6 rip invalid-timer**

Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.

**ipv6 rip invalid-timer seconds**

---

**Syntax Definitions**

```
seconds: Time, in seconds, that a route will remain in an “Active” state. Valid range is 1 - 300.
```

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>180</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This timer is reset each time a routing update is received.

**Examples**

```
-> ipv6 rip invalid-timer 300
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ipv6 rip garbage-timer**: Configures the RIPng garbage timer value.
- **ipv6 rip holddown-timer**: Configures the amount of time a route is placed in a holddown state.

**MIB Objects**

```
alaProtocolripng
   alaRipngInvalidTimer
```
ipv6 rip garbage-timer

Configures the RIPng garbage timer value. When a route in the RIB exceeds the configured Invalid Timer Value, the route is moved to a “Garbage” state in the RIB. The garbage timer is the length of time a route will stay in this state before it is flushed from the RIB.

ipv6 rip garbage-timer seconds

Syntax Definitions

seconds Time, in seconds, that a route will remain in the RIPng Routing Table before it is flushed from the RIB. Valid range is 0 - 180.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>120</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the ipv6 rip invalid-timer command to set the Invalid Timer Value.

Examples

-> ipv6 rip garbage-timer 180

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ipv6 rip invalid-timer`  
  Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.

- `ipv6 rip holddown-timer`  
  Configures the amount of time a route is placed in a holddown state.

**MIB Objects**

```
alaProtocolripng
  alaRipngGarbageTimer
```
ipv6 rip holddown-timer

Configures the amount of time a route is placed in a holddown state. Whenever a route is seen from the same gateway with a higher metric than the route in RIB, the route goes into holddown. This excludes route updates with an INFINITY metric.

**ipv6 rip holddown-timer seconds**

---

**Syntax Definitions**

`seconds` Time, in seconds, that a route will remain in a holddown state. Valid range is 0–120.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

While in holddown, the route continues being announced as usual and used in RIB. This interval is used to control route flap dampening.

---

**Examples**

```
-> ipv6 rip holddown-timer 60
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- **ipv6 rip invalid-timer** Configures the amount of time a route remains active in RIB before being moved to the "Garbage" state.
- **ipv6 rip garbage-timer** Configures the RIPng garbage timer value.

---

**MIB Objects**

alaProtocolripng
ipv6 rip holddown-timer

alaRipngHolddownTimer
ipv6 rip jitter

Configures an offset value for RIPng updates. This is the maximum (positive or negative) value that can be used to offset the update interval. For example, with an update interval of 30 seconds, and a jitter value of 5 seconds, the RIPng update packet would be sent somewhere (random) between 25 and 35 seconds from the previous update.

Syntax:

```
ipv6 rip jitter value
```

**Syntax Definitions**

- **value**: Time, in seconds, that a routing update is offset. Valid range is 0 to one-half the updated interval value (e.g., if the updated interval is 30, the range would be 0–300).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>5</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>upported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

As you increase the number of RIPng interfaces/peers, it is recommended that you increase the Jitter value to reduce the number of RIPng updates being sent over the network.

**Examples**

```
-> ipv6 rip jitter 10
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ipv6 rip update-interval**: Configures the RIPng update interval.
- **show ipv6 rip**: Displays RIPng status and general configuration information.

**MIB Objects**

- `alaProtocolripng`
alaRipngJitter
**ipv6 rip route-tag**

Configures the route tag value for RIP routes generated by the switch.

**ipv6 rip route-tag value**

---

### Syntax Definitions

**value**

Route tag value. Valid range is 0 – 65535.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

This value does not apply to routes learned from other routers. For these routes, the route tag propagates with the route.

---

### Examples

```
-> ipv6 rip route-tag 30
```

---

### Release History

Release 7.1.1; command was introduced.

---

### Related Commands

**show ipv6 rip**

Displays RIPng status and general configuration information.

---

### MIB Objects

**alaProtocolripng**

alaRipngRouteTag
**ipv6 rip update-interval**

Configures the RIPng update interval. This is the interval, in seconds, that RIPng routing updates will be sent out.

**ipv6 rip update-interval seconds**

---

**Syntax Definitions**

- **seconds** Interval, in seconds, that RIPng routing updates are sent out. Valid range is 0–120.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>OS Support</th>
<th>Command Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use this command, along with the **ipv6 rip jitter** command to configure RIPng updates.

---

**Examples**

```
-> ipv6 rip update-interval 30
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- **ipv6 rip jitter** Configures an offset value for RIPng updates.
- **show ipv6 rip** Displays RIPng status and general configuration information.

---

**MIB Objects**

- **alaRipng**
  - **alaRipngUpdateInterval**
ipv6 rip triggered-sends

Configures the behavior of triggered updates.

ipv6 rip triggered-sends {all | updated-only | none}

**Syntax Definitions**

- **all**: All RIPng routes are added to any triggered updates.
- **updated-only**: Only route changes that are causing the triggered update are included in the update packets.
- **none**: RIPng routes are not added to triggered updates.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>updated-only</td>
</tr>
<tr>
<td>updated-only</td>
<td>updated-only</td>
</tr>
<tr>
<td>none</td>
<td>updated-only</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If set to **all**, all routes are sent in the update, not just route changes, which increases RIPng traffic on the network.
- If set to **none**, no triggered updates are sent, which can cause delays in network convergence.

**Examples**

```
-> ipv6 rip triggered-sends none
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show ipv6 rip**: Displays RIPng status and general configuration information.

**MIB Objects**

- `alaProtocolripng`
ipv6 rip interface

Creates or deletes a RIPng interface.

ipv6 rip interface if_name

no ipv6 rip interface if_name

Syntax Definitions

if_name IPv6 interface name.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- By default, a RIPng interface is created in the enabled state.
- Routing is enabled on a VLAN when you create a router port. However, to enable RIPng routing, you must also configure and enable a RIPng routing interface on the VLAN’s IP router port. For more information on VLANs and router ports, see Chapter 5, “VLAN Management Commands”.
- RIPng will support a maximum of 20 interfaces.

Examples

-> ipv6 rip interface Test_Lab

Release History

Release 7.1.1; command was introduced.
Related Commands

- **ipv6 load rip**: Loads RIPng into memory.
- **ipv6 rip admin-state**: Enables or disables RIPng on the switch.
- **ipv6 rip interface recv-status**: Configures IPv6 RIPng interface “Receive” status. When this status is set to "enable", packets can be received on this interface.
- **ipv6 rip interface send-status**: Configures IPv6 RIPng interface “Send” status. When this status is set to "enable", packets can be sent on this interface.
- **show ipv6 rip interface**: Displays information for all or specified RIPng interfaces.

MIB Objects

- **alaRipngInterfaceTable**
  - **alaRipngInterfaceStatus**
ipv6 rip interface metric

Configures the RIPng metric or cost for a specified interface. Priorities for routes generated by a switch can be set by assigning a metric value to routes generated by that switch’s RIPng interface. For example, routes generated by a neighboring switch may have a hop count of 1. However, the priority of routes generated by that switch can be lowered by increasing the metric value for routes generated by the RIPng interface.

ipv6 rip interface if_name metric value

Syntax Definitions

if_name IPv6 interface name.
value Metric value. Valid range is 1 - 15.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

When a metric for a RIPng interface is configured, this metric cost is added to the metric of the incoming route.

Examples

-> ipv6 rip Test_lab metric 1

Release History

Release 7.1.1; command was introduced.
Related Commands

- `ipv6 rip interface` Creates or deletes a RIPng interface.
- `show ipv6 rip interface` Displays information for all or specified RIPng interfaces.

MIB Objects

- `alaRipngInterfaceTable`  
  - `alaRipngInterfaceMetric`
ipv6 rip interface recv-status

Configures IPv6 RIPng interface “Receive” status. When this status is set to “enable”, packets can be received on this interface. When it is set to “disable”, packets will not be received on this interface.

ipv6 rip interface if_name recv-status {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>if_name</th>
<th>IPv6 interface name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the “Receive” status for the specified interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the “Receive” status for the specified interface.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

RIPng must be loaded (ip load rip) and enabled (ipv6 rip admin-state) on the switch to send or receive packets on the interface.

Examples

-> ipv6 rip interface Test_Lab recv-status disable

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ipv6 load rip` Loads RIPng into memory.
- `ipv6 rip admin-state` Enables/disables RIPng on the switch.
- `ipv6 rip interface send-status` Configures IPv6 RIPng interface “Send” status.

**MIB Objects**

- `alaRipngInterfaceTable`  
  - `alaRipngInterfaceRecvStatus`
ipv6 rip interface send-status

Configures IPv6 RIPng interface “Send” status. When this status is enabled, packets can be sent from this interface. When it is disabled, packets will not be sent from this interface.

ipv6 rip interface if_name send-status {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>if_name</th>
<th>IPv6 interface name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the “Send” status for the specified interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the “Send” status for the specified interface.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

RIPng must be loaded (ip load rip) and enabled (ipv6 rip admin-state) on the switch to send or receive packets on the interface.

Examples

-> ipv6 rip interface Test_Lab send-status enable

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **ipv6 load rip**  Loads RIPng into memory.
- **ipv6 rip admin-state**  Enables/disables RIPng on the switch.
- **ipv6 rip interface recv-status**  Configures IPv6 RIPng interface “Receive” status.

**MIB Objects**

alaRipngInterfaceTable
  alaRipngInterfaceSendStatus
**ipv6 rip interface horizon**

Configures the routing loop prevention mechanisms.

`ipv6 rip interface if_name horizon {none | split-only | poison}`

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>if_name</code></td>
<td>IPv6 interface name.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Disables loop prevention mechanisms.</td>
</tr>
<tr>
<td><code>split-only</code></td>
<td>Enables split-horizon, without poison-reverse.</td>
</tr>
<tr>
<td><code>poison</code></td>
<td>Enables split-horizon with poison-reverse.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>split-only</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If set to `none` the route is not sent back to the peer.
- If set to `split-only`, the route received from the peer is sent back with an increased metric.
- If set to `poison` the route received from the peer is sent back with an “infinity” metric.

### Examples

`-> ipv6 rip interface Test_Lab none`

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **show ipv6 rip interface**  Displays information for all or specified RIPng interfaces.
- **show ipv6 rip routes**     Displays all or a specific set of routes in the RIPng Routing Table.

MIB Objects

- **alaRipngInterfaceTable**
  - **alaRipngInterfaceHorizon**
show ipv6 rip

Displays the RIPng status and general configuration parameters.

show ipv6 rip

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```bash
-> show ipv6 rip
Status             = Enabled,
Number of routes   = 10,
Route tag          = 0,
Update interval    = 30,
Invalid interval   = 180,
Garbage interval   = 120,
Holddown interval  = 0,
Jitter interval    = 5,
Triggered Updates  = All Routes,
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>RIPng protocol status (enabled or disabled).</td>
</tr>
<tr>
<td>Number of routes</td>
<td>Number of RIPng routes in Forwarding Information Base (FIB).</td>
</tr>
<tr>
<td>Route tag</td>
<td>Route tag value for RIP routes generated by the switch. Default is 0.</td>
</tr>
<tr>
<td>Invalid interval</td>
<td>Invalid Timer setting, in seconds.</td>
</tr>
<tr>
<td>Garbage interval</td>
<td>Garbage Timer setting, in seconds.</td>
</tr>
<tr>
<td>Holddown interval</td>
<td>Holddown Timer setting, in seconds.</td>
</tr>
</tbody>
</table>
RIP Commands

show ipv6 rip

output definitions

<table>
<thead>
<tr>
<th>Jitter interval</th>
<th>Jitter setting.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggered updates</td>
<td>Triggered Updates setting (All Routes, Updated Routes, and None).</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip admin-state  Enables or disables RIPng routing on the switch.
ipv6 rip route-tag    Configures the route tag value for RIP routes generated by the switch.
ipv6 rip update-interval  Configures the Interval, in seconds, so that RIPng routing updates are sent out.
ipv6 rip invalid-timer  Configures the amount of time a route remains active in RIB before being moved to the "garbage" state.
ipv6 rip holddown-timer  Configures the amount of time a route is placed in a holddown state.
ipv6 rip jitter         Configures an offset value for RIPng updates. This is the maximum (positive or negative) value that can be used to offset the update interval.
ipv6 rip triggered-sends Configures the behavior of triggered updates.

MIB Objects

alaRipngInterfaceTable
  alaRipngInterfaceStatus
  alaRipngRouteTag
  laRipngInvalidTimer
  alaRipngGarbageTimer
  alaRipngHolddownTimer
  alaRipngJitter
  alaRipngTriggeredSends
show ipv6 rip interface

Displays information for all or specified RIPng interfaces.

show ipv6 rip interface [if_name]

Syntax Definitions

if_name IPv6 interface name.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If an interface name is not specified, all IPv6 RIP interfaces are displayed.

Examples

-> show ipv6 rip interface

```
<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Status</th>
<th>Packets Recvd</th>
<th>Packets Sent</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test_Lab</td>
<td>Active</td>
<td>12986</td>
<td>12544</td>
<td>1</td>
</tr>
<tr>
<td>Test_Lab_2</td>
<td>Active</td>
<td>12556</td>
<td>12552</td>
<td>1</td>
</tr>
</tbody>
</table>
```

-> show ipv6 rip interface if3

```
Name = Test_Lab,
IPv6 interface index = 3,
Interface status = Active,
Next Update = 27 secs,
Horizon Mode = Split and Poison-reverse,
MTU size = 1500,
Metric = 1,
Send status = Enabled,
Receive status = Enabled,
Packets received = 12986,
Packets sent = 12544,
```
output definitions

<table>
<thead>
<tr>
<th>Interface name</th>
<th>Interface name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 interface index</td>
<td>IPv6 index of this interface.</td>
</tr>
<tr>
<td>Status</td>
<td>Interface status (Active/Inactive).</td>
</tr>
<tr>
<td>Packets Recvd</td>
<td>Number of packets received by the interface.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Number of packets sent by the interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>RIPng metric (cost) configured for the interface.</td>
</tr>
<tr>
<td>IPv6 interface index</td>
<td>IPv6 interface index number.</td>
</tr>
<tr>
<td>Interface status</td>
<td>Interface status (Active/Inactive).</td>
</tr>
<tr>
<td>Next update</td>
<td>Seconds remaining until the next update on this interface.</td>
</tr>
<tr>
<td>Horizon mode</td>
<td>Interface Horizon Mode (routing loop prevention mechanisms).</td>
</tr>
<tr>
<td></td>
<td>Displayed modes are none/split-only/poison-reverse.</td>
</tr>
<tr>
<td>MTU size</td>
<td>Maximum transmission size for RIPng packets on the interface.</td>
</tr>
<tr>
<td>Send status</td>
<td>Interface “Send” status. When this status is set to &quot;enable&quot;, packets can be sent from this interface. When it is set to &quot;disable&quot;, packets will not be sent from this interface.</td>
</tr>
<tr>
<td>Receive status</td>
<td>Interface “Receive” status. When this status is set to &quot;enable&quot;, packets can be received by this interface. When it is set to &quot;disable&quot;, packets cannot be received by this interface.</td>
</tr>
<tr>
<td>Packets received</td>
<td>Number of packets received by the interface.</td>
</tr>
<tr>
<td>Packets sent</td>
<td>Number of packets sent by the interface.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 rip interface       IPv6 interface name.
ipv6 rip admin-state     Enables or disables RIPng routing on the switch.
ipv6 rip interface recv-status Configures the interface “Receive” status. When this status is set to "enable", packets can be received by this interface. When it is set to "disable", packets cannot be received by this interface.
ipv6 rip interface send-status Configures the interface “Send” status. When this status is set to "enable", packets can be sent from this interface. When it is set to "disable", packets will not be sent from this interface.
ipv6 rip interface metric Configures the RIPng metric (cost) for the interface.
ipv6 rip interface horizon Configures the interface Horizon Mode (routing loop prevention mechanisms).
show ipv6 rip             Displays RIPng status and general configuration parameters (e.g., force holddown timer).
MIB Objects

alaRipngInterfaceTable
   alaRipngInterfaceEntry
   alaRipngInterfaceStatus
   alaRipngInterfacePacketsRcvd
   alaRipngInterfacePacketsSent
   alaRipngInterfaceMetric
   alaRipngInterfaceIndex
   alaRipngInterfaceNextUpdate
   alaRipngInterfaceHorizon
   alaRipngInterfaceMTU
   alaRipngInterfaceSendStatus
   alaRipngInterfaceRecvStatus
show ipv6 rip peer

Displays a summary of the observed RIPng peers, or specific information about a peer when a peer address is provided.

show ipv6 rip peer [ipv6_addresss]

Syntax Definitions

ipv6_addresss  IPv6 address of the peer.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you do not specify a peer, all IPv6 RIP peers are displayed.

Examples

-> show ipv6 peer

<table>
<thead>
<tr>
<th>Address</th>
<th>Seen on Interface</th>
<th>Packets</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::200:39ff:fe1f:710c</td>
<td>vlan172</td>
<td>23</td>
<td>20</td>
</tr>
<tr>
<td>fe80::2d0:95ff:fe12:da40</td>
<td>bkbone20</td>
<td>33</td>
<td>2</td>
</tr>
<tr>
<td>fe80::2d0:95ff:fe12:da40</td>
<td>vlan150</td>
<td>26</td>
<td>25</td>
</tr>
<tr>
<td>fe80::2d0:95ff:fe6a:5d41</td>
<td>nssa23</td>
<td>20</td>
<td>25</td>
</tr>
</tbody>
</table>

-> show ipv6 rip peer fe80::2d0:95ff:fe12:da40

Peer#1 address = fe80::2d0:95ff:fe12:da40,
Seen on interface = bkbone20,
Last Update = 8 secs,
Received packets = 33,
Received bad packets = 0,
Received routes = 5,
Received bad routes = 0

Peer#2 address = fe80::2d0:95ff:fe12:da40,
Seen on interface = vlan150,
Last Update = 1 secs,
Received packets = 27,
Received bad packets = 0,
Received routes = 2,
Received bad routes = 0
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IPv6 address of the peer.</td>
</tr>
<tr>
<td>Seen on Interface</td>
<td>Interface used to reach the peer.</td>
</tr>
<tr>
<td>Packets Recvd</td>
<td>Number of packets received from the peer.</td>
</tr>
<tr>
<td>Last Update</td>
<td>Number of seconds since the last update was received from the peer.</td>
</tr>
<tr>
<td>Peer address</td>
<td>Peer IPv6 address.</td>
</tr>
<tr>
<td>Received packets</td>
<td>Number of packets received from the peer.</td>
</tr>
<tr>
<td>Received bad packets</td>
<td>Number of bad packets received from the peer.</td>
</tr>
<tr>
<td>Received routes</td>
<td>Number of RIPng routes received from the peer.</td>
</tr>
<tr>
<td>Received bad routes</td>
<td>Number of bad RIPng routes received from the peer.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

- `show ipv6 rip interface`  Displays all or specified RIPng interface status.
- `show ipv6 rip routes`    Displays all or a specific set of routes in RIPng Routing Table.

MIB Objects

alaRipngPeerTable
  alaRipngPeerEntry
  alaRipngPeerAddress
  alaRipngPeerIndex
  alaRipngPeerLastUpdate
  alaRipngPeerNumUpdates
  alaRipngPeerBadPackets
  alaRipngPeerNumRoutes
  alaRipngPeerBadRoutes
show ipv6 rip routes

Displays all or a specific set of routes in RIPng Routing Table.

show ipv6 rip routes [dest ipv6_prefix/prefix_length | gateway ipv6_addr | detail ipv6 prefix/prefix_length]

Syntax Definitions

dest Displays all routes whose destination matches the IPv6 prefix/prefix length.
gateway Displays all routes whose gateway matches the specified IPv6 address.
detail Displays detailed information about a single route matching the specified destination.
ipv6_prefix/prefix length IPv6 address and prefix/prefix length.
ipv6_addr IPv6 address.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If none of the optional parameters are entered with this command, all IPv6 RIP routes are displayed.

Examples

-> show ipv6 rip routes

Legends: State: A = Active, H = Holddown, G = Garbage

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>State</th>
<th>Metric</th>
<th>Proto</th>
</tr>
</thead>
<tbody>
<tr>
<td>100::1/128</td>
<td>+fe80::200:39ff:fe1f:710c</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td>100::100/1/128</td>
<td>+fe80::200:39ff:fe1f:710c</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td>400::/100</td>
<td>+fe80::2d0:95ff:fe12:e050</td>
<td>A</td>
<td>1</td>
<td>Local</td>
</tr>
<tr>
<td>900::/100</td>
<td>+fe80::2d0:95ff:fe12:e050</td>
<td>A</td>
<td>1</td>
<td>Local</td>
</tr>
<tr>
<td>8900::/100</td>
<td>+fe80::2d0:95ff:fe12:da40</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td>9800::/100</td>
<td>+fe80::2d0:95ff:fe12:da40</td>
<td>A</td>
<td>2</td>
<td>Rip</td>
</tr>
<tr>
<td>9900::/100</td>
<td>+fe80::2d0:95ff:fe12:e050</td>
<td>A</td>
<td>1</td>
<td>Local</td>
</tr>
</tbody>
</table>
-> show ipv6 rip routes detail 9900::/100

Destination = 9900::,
Mask length = 100,
Gateway(1) = fe80::2d0:95ff:fe12:e050,
Protocol = Local,
Out Interface = nssa23,
Metric = 1,
Status = Installed,
State = Active,
Age = 10544s,
Tag = 0,
Gateway(2) = fe80::2d0:95ff:fe12:da40,
Protocol = Rip,
Out Interface = bkbone20,
Metric = 2,
Status = Not Installed,
State = Active,
Age = 15s,
Tag = 0,

output definitions

<table>
<thead>
<tr>
<th>Destination</th>
<th>IPv6 address/address length of the destination.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>IPv6 gateway used to reach the destination.</td>
</tr>
<tr>
<td>State</td>
<td>Route status (Active/Inactive).</td>
</tr>
<tr>
<td>Metric</td>
<td>Routing metric for this route.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used to learn the route.</td>
</tr>
<tr>
<td>Mask Length</td>
<td>Prefix Length.</td>
</tr>
<tr>
<td>Out Interface</td>
<td>The interface used to reach the destination.</td>
</tr>
<tr>
<td>Status</td>
<td>Route status (Active/Inactive).</td>
</tr>
<tr>
<td>Age</td>
<td>The number of seconds since the route was last updated.</td>
</tr>
<tr>
<td>Tag</td>
<td>The route tag value for the route.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ipv6 rip interface`  Creates/deletes a RIPng interface.
- `ipv6 rip interface metric`  Configures the RIPng metric or cost for a specified interface.
- `show ipv6 rip interface`  Displays all or specified RIPng interface status.

**MIB Objects**

- `alaRipngRouteTable`
- `alaRipngRouteEntry`
- `alaRipngRoutePrefixLen`
- `alaRipngRouteNextHop`
- `alaRipngRouteType`
- `alaRipngRouteAge`
- `alaRipngRouteTag`
- `alaRipngRouteStatus`
- `alaRipngRouteMetric`
Bidirectional Forwarding Detection (BFD) is a hello protocol, which can be configured to interact with routing protocols for the detection of path failures and can reduce the convergence time in a network. BFD is supported with the BGP, IS-IS, OSPF, PIM, VRRP, and Static Routes.

When BFD is configured and enabled, BFD sessions are created and timers are negotiated between BFD neighbors. If a system does not receive a BFD control packet within the negotiated time interval, the neighbor system is considered down. Rapid failure detection notices are then sent to the routing protocol, which initiates a routing protocol recalculation. This process can reduce the time of convergence in a network.

This implementation of BFD supports an Asynchronous control packet mode or an Asynchronous Echo function. Demand mode is not supported.

- When the Asynchronous control packet mode is activated, BFD neighbors periodically send BFD control packets to each other. A time interval for transmitting and receiving such packets is negotiated between the two BFD systems. If a neighboring system fails to receive a number of control packets continuously over a specific period of time, the session is considered down and BFD informs the appropriate routing protocol.

- The Asynchronous Echo function is used to verify the forwarding path between neighboring BFD systems. When active, a BFD system transmits Echo packets only (no control packets are sent) to a BFD neighbor, which then sends the packets back to the originating system along the forwarding path. If no Echo packets are received back from the BFD neighbor within a configured Echo time interval, the session is considered down.

MIB information for the BFD commands is as follows:

```
Filename:   ALCATEL-IND1-BFD-MIB.mib
Module:     alcatelIND1BfdMIB
```

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>Global BFD commands</th>
<th>IP BFD commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip bfd admin-state</td>
<td>ip bfd admin-state</td>
</tr>
<tr>
<td>ip bfd transmit</td>
<td>ip bfd transmit</td>
</tr>
<tr>
<td>ip bfd receive</td>
<td>ip bfd receive</td>
</tr>
<tr>
<td>ip bfd multiplier</td>
<td>ip bfd multiplier</td>
</tr>
<tr>
<td>ip bfd echo-interval</td>
<td>ip bfd echo-interval</td>
</tr>
<tr>
<td>show ip bfd</td>
<td>show ip</td>
</tr>
<tr>
<td></td>
<td>show ip</td>
</tr>
<tr>
<td></td>
<td>BFD Interface commands</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>ip</td>
</tr>
<tr>
<td></td>
<td>show ip</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 24-1
ip bfd admin-state

Enables or disables the global BFD protocol status for the switch.

ip bfd admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD.</td>
</tr>
</tbody>
</table>

Defaults

By default, BFD is disabled for the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Disabling BFD does not remove the existing BFD configuration from the switch.
- When BFD is disabled, all BFD functionality is disabled for the switch, but configuring BFD is still allowed.
- Configuring BFD global parameters is not allowed when BFD is enabled for the switch.

Examples

-> ip bfd admin-state enable
-> ip bfd admin-state disable

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bfd

Displays the BFD global status and general configuration parameters.

MIB Objects

alaBfdGlobalAdminStatus
**ip bfd transmit**

Configures the global transmit time interval for BFD control packets. This command specifies the minimum amount of time BFD waits between each transmission of control packets.

```
ip bfd transmit transmit_interval
```

**Syntax Definitions**

`transmit_interval` The transmit time interval, in milliseconds. The valid range is 100–999.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>transmit_interval</code></td>
<td>300 milliseconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The transmit time interval is also configurable at the BFD interface level. Note that configuring the global value with the `ip bfd transmit` command does not override the value set for the interface using the `ip bfd interface transmit` command.

- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

**Examples**

```
-> ip bfd transmit 500
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `ip|ipv6 bfd interface transmit`  Configures the transmit time interval for a specific BFD interface.
- `show ip bfd`  Displays the BFD global status and general configuration parameters.

MIB Objects

- `alaBfdGlobalTxInterval`
ip bfd receive

Configures the global receive time interval for BFD control packets. This command specifies the minimum amount of time BFD waits to receive control packets before determining there is a problem.

```
ip bfd receive receive_interval
```

**Syntax Definitions**

```
receive_interval
```

The receive time interval, in milliseconds. The valid range is 100–999.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>receive_interval</td>
<td>300 milliseconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The minimum receive time interval is also configurable at the BFD interface level. Note that configuring the global value with the `ip bfd receive` command does not override the value set for the interface using the `ip bfd interface receive` command.

- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

**Examples**

```
-> ip bfd receive 500
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip|ipv6 bfd interface receive**  Configures the receive time interval for a specific BFD interface.
- **show ip bfd**  Displays the BFD global status and general configuration parameters.

MIB Objects

- **alaBfdGlobalRxInterval**
**ip bfd multiplier**

Configures the global BFD detection time multiplier. This command specifies a number that is used to calculate the BFD detection time used in the asynchronous mode. The detection time value that is specified determines how long to wait before declaring that the BFD session is down.

```plaintext
ip bfd multiplier num
```

**Syntax Definitions**

`num` The detection time multiplier number. The valid range is 3–255.

**Defaults**

By default, the multiplier value is set to 3.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- The global detection time multiplier is also configurable at the BFD interface level. Note that configuring the global value with the `ip bfd multiplier` command does not override the value set for the interface using the `ip bfd interface multiplier` command.

- The global detection time multiplier serves as the default multiplier value for a BFD interface. The default multiplier value is overridden when a specific value is configured for the interface.

**Examples**

`-> ip bfd multiplier 5`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip|ipv6 bfd interface multiplier`  Configures the detection time multiplier for a BFD interface.
- `show ip bfd`  Displays the BFD global status and general configuration parameters.

**MIB Objects**

- `alaBfdGlobalDetectMult`
**ip bfd echo-interval**

Configures the global BFD echo packet time interval. The echo function is available with the asynchronous mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

**ip bfd echo-interval** *echo_interval*

---

**Syntax Definitions**

*echo_interval*  
The echo time interval, in milliseconds. The valid range is 100–999.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>echo_interval</em></td>
<td>300 milliseconds</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The echo packet time interval is also configurable at the BFD interface level. Note that configuring the global value with the **ip bfd echo-interval** command does not override the value set for the interface using the **ip bfd interface echo-interval** command.

- The global echo packet time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

---

**Examples**

```
-> ip bfd echo-interval 500
```

---

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip|ipv6 bfd interface echo-interval`  
  Configures the echo packet time interval for a BFD interface.

- `show ip bfd`  
  Displays the BFD global status and general configuration parameters.

**MIB Objects**

- `alaBfdGlobalEchoRxInterval`
**ip|ipv6 bfd interface**

Configures an IPv4 or IPv6 BFD interface.

```
{ip | ipv6} bfd interface if_name
no {ip | ipv6} bfd interface if_name
```

**Syntax Definitions**

`if_name`  
The name of an existing IPv4 or IPv6 interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete a BFD interface.
- The interface name must be an existing IPv4 or IPv6 interface name that is configured with an IPv4 or IPv6 address.

**Examples**

```
-> ip bfd interface bfd-vlan-101
-> no ip bfd interface bfd-vlan-101

-> ipv6 bfd interface bfd-vlan-201
-> no ipv6 bfd interface bfd-vlan-201
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.
**Related Commands**

- `ip|ipv6 bfd interface admin-state`
  - Configures the administrative status of an IPv4 or IPv6 BFD interface.
- `show ip|ipv6 bfd interfaces`
  - Displays the status and statistics of a BFD interface.
- `show ip|ipv6 bfd sessions`
  - Displays the status and statistics of the BFD sessions.

**MIB Objects**

- `alaBfdIntfTable`
  - `alaBfdIntfIndex`
  - `alaBfdIntfRowStatus`
**ip|ipv6 bfd interface admin-state**

Enables or disables the administrative status of an IPv4 or IPv6 BFD interface.

```
{ip | ipv6} bfd interface if_name admin-state {enable | disable}
```

**Syntax Definitions**

- `if_name` The name of an existing IPv4 or IPv6 BFD interface.
- `enable` Enables the BFD interface.
- `disable` Disables the BFD interface.

**Defaults**

By default, a BFD interface is disabled when it is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BFD interface must be enabled to participate in the BFD protocol.

**Examples**

- `-> ip bfd interface bfd-vlan-101 admin-state enable`
- `-> ip bfd interface bfd-vlan-101 admin-state disable`
- `-> ipv6 bfd interface bfd-vlan-201 admin-state enable`
- `-> ipv6 bfd interface bfd-vlan-201 admin-state disable`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.
**Related Commands**

- `ip|ipv6 bfd interface`  
  Creates an IPv4 or IPv6 BFD interface.

- `show ip|ipv6 bfd interfaces`  
  Displays the status and statistics of a BFD interface.

- `show ip|ipv6 bfd sessions`  
  Displays the status and statistics of BFD sessions.

**MIB Objects**

- `alaBfdIntfTable`  
  
  - `alaBfdIntfAdminStatus`
**ip|ipv6 bfd interface transmit**

Configures the transmit time interval for an IPv4 or IPv6 BFD interface. This command specifies the minimum amount of time BFD waits between each transmission of control packets from the interface.

```
{ip | ipv6} bfd interface if_name transmit transmit_interval
```

### Syntax Definitions

- `if_name` The name of an existing IPv4 or IPv6 BFD interface.
- `transmit_interval` The transmit time interval, in milliseconds. The valid range is 100–999.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>transmit_interval</td>
<td>300 milliseconds</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The global transmit time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.
- Note that configuring the interface transmit time interval using the `ip bfd interface transmit` or `ipv6 bfd interface transmit` command does not change the global value configured with the `ip bfd transmit` command.

### Examples

```
-> ip bfd interface bfd-vlan-101 transmit 500
```

```
-> ipv6 bfd interface bfd-vlan-201 transmit 500
```

### Release History

- Release 7.1.1; command was introduced.
- Release 8.4.1.R03; IPv6 BFD support added.
**Related Commands**

- `ip|ipv6 bfd interface`  Creates an IPv4 or IPv6 BFD interface.
- `ip bfd transmit`        Configures a global BFD transmit time interval.
- `show ip|ipv6 bfd interfaces`  Displays the status and statistics of a BFD interface.
- `show ip|ipv6 bfd sessions` Displays the status and statistics of the BFD sessions.

**MIB Objects**

- `alaBfdIntfTable`
  - `alaBfdIntfDesiredMinTxInterval`
ip|ipv6 bfd interface receive

Configures the receive time interval for an IPv4 or IPv6 BFD interface. This command specifies the minimum amount of time BFD waits to receive control packets on the interface before determining there is a problem.

{ip | ipv6} bfd interface if_name receive receive_interval

Syntax Definitions

if_name
   The name of an existing IPv4 or IPv6 BFD interface.

receive_interval
   The receive time interval, in milliseconds. The valid range is 100–999.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>receive_interval</td>
<td>300 milliseconds</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C4E/V48C8/C32E/T24C2/</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The global receive time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

- Note that configuring the interface transmit time interval using the ip bfd interface receive or ipv6 bfd interface receive command does not change the global value configured with the ip bfd receive command.

Examples

- ip bfd interface bfd-vlan-101 receive 500
- ipv6 bfd interface bfd-vlan-201 receive 500

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.
**Related Commands**

- **ip|ipv6 bfd interface**
  Creates an IPv4 or IPv6 BFD interface.
- **ip bfd receive**
  Configures a global BFD receive time interval.
- **show ip|ipv6 bfd interfaces**
  Displays the BFD interface configuration table.
- **show ip|ipv6 bfd sessions**
  Displays the BFD interface configuration table.

**MIB Objects**

- **alaBfdIntfTable**
  - **alaBfdReqMinRxInterval**
ip|ipv6 bfd interface multiplier

Configures the detection time multiplier for an IPv4 or IPv6 BFD interface. This command specifies a number that is used to calculate the BFD detection time used in the asynchronous mode. When an interface stops receiving packets from a neighbor, the interface uses the detection time value to determine how long to wait before declaring that the BFD session is down.

```
{ip | ipv6} bfd interface if_name multiplier num
```

**Syntax Definitions**

- `if_name` - The name of an existing IPv4 or IPv6 BFD interface.
- `num` - The detection time multiplier number. The valid range is 3–255.

**Defaults**

By default, the multiplier value is set to 3.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The detection time between neighbors is calculated by multiplying the negotiated transmit time interval by the detection time multiplier.

**Examples**

```
-> ip bfd interface bfd-vlan-101 multiplier 5
-> ipv6 bfd interface bfd-vlan-201 multiplier 5
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.
Related Commands

- **ip|ipv6 bfd interface**: Creates an IPv4 or IPv6 BFD interface.
- **show ip|ipv6 bfd interfaces**: Displays the BFD interface configuration table.
- **show ip|ipv6 bfd sessions**: Displays the BFD interface configuration table.

MIB Objects

- **alaBfdIntfTable**
  - **alaBfdIntfDetectMult**
ip|ipv6 bfd interface echo-interval

Configures the echo time interval for an IPv4 or IPv6 BFD interface. The echo function is available with the asynchronous mode. Echo packets are transmitted to BFD peers to see if they loop back to the peer from which they originated.

{ip | ipv6} bfd interface if_name echo-interval echo_interval

Syntax Definitions

if_name
The name of an existing IPv4 or IPv6 BFD interface.

echo_interval
The echo time interval, in milliseconds. The valid range is 100–999.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo_interval</td>
<td>300 milliseconds</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32 No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The global echo time interval serves as the default interval value for a BFD interface. The default interval value is overridden when a specific value is configured for the interface.

- Note that configuring the interface echo time interval using the ip bfd interface echo-interval or ipv6 bfd interface echo-interval command does not change the global value configured with the ip bfd echo-interval command.

Examples

- ip bfd interface bfd-vlan-101 echo-interval 500
- ip bfd interface bfd-vlan-201 echo-interval 500

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.
**Related Commands**

- **ip|ipv6 bfd interface**  
  Creates an IPv4 or IPv6 BFD interface.

- **ip bfd echo-interval**  
  Configures a global BFD echo time interval.

- **show ip|ipv6 bfd interfaces**  
  Displays the BFD interface configuration table.

- **show ip|ipv6 bfd sessions**  
  Displays the BFD interface configuration table.

**MIB Objects**

- **alaBfdIntfTable**
  - **alaBfdIntfReqMinEchoRxInterval**
show ip bfd

Displays the global BFD configuration table.

show ip bfd

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ip bfd
BFD Version Number     = 1,
Admin Status           = Enabled,
Desired Transmit Interval = 300,
Minimum Receive Interval = 300,
Detection Time Multiplier = 3,
Minimum Echo Receive Interval = 300,
Applications Registered = STATIC-ROUTING OSPF

Output definitions

<table>
<thead>
<tr>
<th>BFD Version Number</th>
<th>Refers to BFD version.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>Refers to BFD global admin status.</td>
</tr>
<tr>
<td>Desired Transmit Interval</td>
<td>Refers to BFD global Tx interval.</td>
</tr>
<tr>
<td>Minimum Receive Interval</td>
<td>Refers to BFD global Rx interval.</td>
</tr>
<tr>
<td>Detection Time Multiplier</td>
<td>Refers to the BFD Detection Time multiplier number.</td>
</tr>
<tr>
<td>Minimum Echo Receive Interval</td>
<td>Refers to BFD echo Rx interval.</td>
</tr>
<tr>
<td>Applications Registered</td>
<td>Refers to applications registered to BFD.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bfd admin-state**  
  Configures BFD at global level.
- **ip|ipv6 bfd interface**  
  Configures BFD at interface level.

**MIB Objects**

- alaBfdIntfTable
  - alaBfdGlobalVersionNumber
  - alaBfdGlobalAdminStatus
  - alaBfdGlobalTxInterval
  - alaBfdGlobalRxInterval
  - alaBfdGlobalDetectMult
  - alaBfdGlobalEchoRxInterval
  - alaBfdGlobalProtocolApps
show ip|ipv6 bfd interfaces

Displays the BFD interface configuration table.

show {ip | ipv6} bfd interfaces [if_name]

**Syntax Definitions**

if_name

The name of the IPv4 or IPv6 BFD interface.

**Defaults**

By default, the configuration for all IPv4 or IPv6 BFD interfaces is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enter an interface name to display information for a specific BFD interface.

**Examples**

-> show ip bfd interfaces
  Interface     Admin     Tx  Min Rx  Min EchoRx Detect  OperStatus
  Name          Status     Interval Interval Interval   Multiplier
  -----------------+----------+----------+----------+----------+----------+----------
  bfd-intf1       enabled   300     300       300         3         UP
  bfd-intf2       enabled   300     300       300         3         UP

-> show ip bfd interfaces bfd-intf1
  Interface Name       = bfd-intf1,
  Interface IP Address = 100.1.1.1,
  Admin Status         = Enabled,
  Desired Transmit Interval = 300,
  Minimum Receive Interval = 300,
  Detection Time Multiplier = 3,
  Minimum Echo Receive Interval = 300,
  Authentication Present = No,
  Oper Status = UP

-> show ipv6 bfd interfaces
  Interface     Admin     Tx  Min Rx  Min EchoRx Detect  OperStatus
  Name          Status     Interval Interval Interval   Multiplier
  -----------------+----------+----------+----------+----------+----------+----------
  bfd-intf3       disabled    300     300       300         3         DOWN
show ipv6 bfd interfaces bfd-intf3

Interface Name                   = bfd-intf3
Interface IP Address             = fe80::2efa:a2ff:fe13:e402,
Admin Status                     = Disabled,
Desired Transmit Interval        = 300,
Minimum Receive Interval         = 300,
Detection Time Multiplier        = 3,
Minimum Echo Receive Interval    = 300,
Authentication Present           = No,
Oper Status                      = DOWN

**output definitions**

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Refers to BFD Interface name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface IP Address</td>
<td>Refers to the IPv4 or IPv6 network address assigned to the BFD interface.</td>
</tr>
<tr>
<td>Admin status</td>
<td>Refers to BFD interface admin status.</td>
</tr>
<tr>
<td>Desired Transmit Interval</td>
<td>Refers to BFD interface Tx interval.</td>
</tr>
<tr>
<td>Minimum Receive Interval</td>
<td>Refers to BFD interface Rx interval.</td>
</tr>
<tr>
<td>Detection Time Multiplier</td>
<td>Refers to BFD interface Detection Time Multiplier.</td>
</tr>
<tr>
<td>Minimum Echo Receive Interval</td>
<td>Refers to BFD interface echo Rx interval.</td>
</tr>
<tr>
<td>Authentication Present</td>
<td>Refers to availability of BFD message authentication on the BFD interface.</td>
</tr>
<tr>
<td>Oper Status</td>
<td>Refers to BFD interface operational status.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

**Related Commands**

- ip bfd admin-state       Configures BFD at global level.
- ip|ipv6 bfd interface     Configures BFD at interface level.

**MIB Objects**

alaBfdIntfTable
  alaBfdIntfIfName
  alaBfdIntfAddr
  alaBfdIntfAdminStatus
  alaBfdIntfDesiredMinTxInterval
  alaBfdIntfRegMinRxInterval
  alaBfdIntfDetectMult
  alaBfdIntfRegMinEchoRxInterval
  alaBfdIntfAuthPresFlag
  alaBfdIntfOperStatus
show ip|ipv6 bfd sessions

Displays the IPv4 or IPv6 BFD sessions for the switch.

**show {ip | ipv6} bfd sessions [session_num] [slot chassis/slot]**

### Syntax Definitions

- **session_num**: The BFD session number. Valid range is 1–1024.
- **chassis**: The chassis identifier.
- **slot**: The current slot position used by the switch.

### Defaults

By default, all IPv4 or IPv6 BFD sessions are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Specify a session number to display information for an individual BFD session.

### Examples

```
-> show ip bfd sessions
Legends: Neg. = Negotiated
         Discr = Discriminator
         Intvl = Interval (in milliseconds)

Local Interface Discr Name      Neighbor State Discr Intvl Intvl Intvl Intvl
              Name      Address            Discr   Intvl   Intvl   Intvl   Intvl
-----------+------------+------------------------+-------+-------+-------+-------+--------
1          one        100.1.1.10    UP     0    0    0   ECHO
2          one        101.1.1.11    UP   10   300   300  ASYNC
```

```
-> show ip bfd sessions slot 1
Legends: Neg. = Negotiated
         Discr = Discriminator
         Intvl = Interval (in milliseconds)

Local Interface Discr Name      Neighbor State Discr Intvl Intvl Intvl Intvl
              Name      Address            Discr   Intvl   Intvl   Intvl   Intvl
-----------+------------+------------------------+-------+-------+-------+-------+--------
1          one        100.1.1.10    UP     0    0    0    300
```


-> show ip bfd sessions 1
Local discriminator              = 1,
Neighbor IP Address              = 100.1.1.10,
Requested Session Type           = ECHO,
Interface IP Address             = 100.1.1.1,
Source UDP Port                  = 49152,
State                            = UP,
Session Operating Mode           = ECHO only,
Remote discriminator             = 0,
Negotiated Tx interval           = 0,
Negotiated Rx interval           = 0,
Echo Rx interval                 = 300,
Multiplier                       = 3,
Applications Registered:         = STATIC-ROUTING

-> show ipv6 bfd sessions
Legends: Neg.     = Negotiated
                  Discr    = Discriminator
                  Intvl    = Interval (in milliseconds)
Local Interface Discr Name Neighbor Address State Discr Intvl Intvl Intvl
-------+---------+-------------------------+-------+-------+-------+-------+--------
1      bfd-intf3 fe80::2efa:a2ff:fe13:e403 UP 0 0 0 300

-> show ipv6 bfd sessions 1
Local discriminator              = 1,
Neighbor IP Address              = fe80::2efa:a2ff:fe13:e402,
Requested Session Type           = ECHO,
Interface IP Address             = fe80::2efa:a2ff:fe13:e403,
Source UDP Port                  = 49152,
State                            = UP,
Session Operating Mode           = ECHO only,
Remote discriminator             = 0,
Negotiated Tx interval           = 0,
Negotiated Rx interval           = 0,
Echo Rx interval                 = 300,
Multiplier                       = 3,
Applications Registered:         = STATIC-ROUTING

**output definitions**

<table>
<thead>
<tr>
<th><strong>Local discriminator</strong></th>
<th>The local discriminator.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Neighbor IP address</strong></td>
<td>The IPv4 or IPv6 address of the BFD neighbor.</td>
</tr>
<tr>
<td><strong>Requested Session Type</strong></td>
<td>The bit map of the session type that is requested.</td>
</tr>
<tr>
<td><strong>Interface IP address</strong></td>
<td>The IPv4 or IPv6 address of the outgoing BFD interface for this session.</td>
</tr>
<tr>
<td><strong>Source UDP Port</strong></td>
<td>The unique source UDP port used to send BFD packets for this session.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>The state of the BFD session.</td>
</tr>
<tr>
<td><strong>Session Operating Mode</strong></td>
<td>The current operating mode of the BFD session.</td>
</tr>
<tr>
<td><strong>Remote discriminator</strong></td>
<td>The remote discriminator.</td>
</tr>
<tr>
<td><strong>Negotiated Tx interval</strong></td>
<td>The negotiated transmit interval.</td>
</tr>
<tr>
<td><strong>Negotiated Rx interval</strong></td>
<td>The negotiated receive interval.</td>
</tr>
<tr>
<td><strong>Echo Rx interval</strong></td>
<td>The Echo packet receive interval.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Detection Time Multiplier</th>
<th>The BFD Detection Time multiplier number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications Registered</td>
<td>The bit map object of applications that are registered with this BFD session.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.

**Related Commands**

- `ip bfd admin-state` Configures BFD at global level.
- `ip|ipv6 bfd interface` Configures BFD at interface level.
- `show ip|ipv6 bfd sessions statistics` Displays the statistics for all BFD sessions.

**MIB Objects**

- `alaBfdSessTable`
  - `alaBfdSessDiscriminator`
  - `alaBfdSessNeighborAddr`
  - `alaBfdSessSessionType`
  - `alaBfdSessIfIndex`
  - `alaBfdSessUdpPort`
  - `alaBfdSessState`
  - `alaBfdSessOperMode`
  - `alaBfdSessDiscriminator`
  - `alaBfdSessNegotiatedTxInterval`
  - `alaBfdSessNegotiatedRxInterval`
  - `alaBfdSessEchoRxInterval`
  - `alaBfdSessDetectMult`
  - `alaBfdSessProtocolApps`
show ip|ipv6 bfd sessions statistics

Displays the statistics for IPv4 or IPv6 BFD sessions.

show {ip | ipv6} bfd sessions statistics [session_num]

Syntax Definitions

session_num The BFD session number. Valid range is 1–1024.

Defaults

By default, statistics for all IPv4 or IPv6 sessions are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify a BFD session number to display statistics for an individual session.

Examples

-> show ip bfd sessions statistics
Legends:
noDiag = noDiagnostic(0)     ctlDetExp = controlDetectionTimeExpired(1)
echFail = echoFunctionFailed(2) nvrDwn = neighborSignaledSessionDown(3)
fwdPlRst = forwardingPlaneReset(4) pthDwn = pathDown(5)
conPthDwn = concatenatedPathDown(6) admDwn = administrativelyDown(7)
rctPthDwn = reverseConcatenatedPathDown(8)

<table>
<thead>
<tr>
<th>Local Discr</th>
<th>Neighbor Address</th>
<th>Tx Packets</th>
<th>Rx Packets</th>
<th>Echo Tx Packets</th>
<th>Last Down Diagnostic Code</th>
<th>Up Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100.1.1.10</td>
<td>0</td>
<td>0</td>
<td>5772</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>101.1.1.11</td>
<td>5242</td>
<td>5241</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

-> show ip bfd sessions statistics 1
Tx packet counter = 0,
Rx packet counter = 0,
Tx Echo packet counter = 5772,
Rx Echo packet counter = 5774,
Session Up Time = 6160400,
Session Down Time = 0,
Last Down Diagnostic Code = 0,
Session Up Count = 1
-> show ipv6 bfd sessions statistics

Legends:
- noDiag = noDiagnostic(0)
- ctlDetExp = controlDetectionTimeExpired(1)
- echFail = echoFunctionFailed(2)
- nbrDwn = neighborSignaledSessionDown(3)
- fwdPlRst = forwardingPlaneReset(4)
- pthDwn = pathDown(5)
- conPthDwn = concatenatedPathDown(6)
- admDwn = administrativelyDown(7)
- rctPthDwn = reverseConcatenatedPathDown(8)

<table>
<thead>
<tr>
<th>Local Discr</th>
<th>Neighbor Address</th>
<th>Tx Packets</th>
<th>Rx Packets</th>
<th>Echo Tx Packets</th>
<th>Last Down Diag Code</th>
<th>Up Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>fe80::2efa:a2ff:fe13:e402</td>
<td>0</td>
<td>0</td>
<td>5772</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Output definitions:
- **Local Discr**: The local discriminator.
- **Neighbor address**: The IP address of the BFD neighbor.
- **Tx Packets**: Number of BFD Control packets transmitted on this session.
- **Rx Packets**: Number of BFD Control packets received on this session.
- **Echo Tx Packets**: Number of BFD Echo packets transmitted on this session.
- **Last Down Diag Code**: Diagnostic code for last session down event.
- **Up Count**: Number of times the session has moved to an UP state since the system was last reset or initialized.

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.
Related Commands

**ip bfd admin-state**
Configures BFD at global level.

**ipv6 bfd interface**
Configures BFD at interface level.

**show ipv6 bfd sessions**
Displays the IPv4 or IPv6 BFD sessions for the switch.

MIB Objects

alaBfdSessPerfTable
- alaBfdSessPerfPktIn
- alaBfdSessPerfPktOut
- alaBfdSessPerfEchoOut
- alaBfdSessPerfEchoIn
- alaBfdSessPerfUpTime
- alaBfdSessPerfLastSessDownTime
- alaBfdSessPerfLastCommLostDiag
- alaBfdSessPerfSessUpCount
- alaBfdSessPerfDiscTime
Bootstrap Protocol (BOOTP) and Dynamic Host Configuration Protocol (DHCP) packets contain configuration information for network hosts. DHCP Relay enables forwarding of BOOTP/DHCP packets between networks. This allows routing of DHCP traffic between clients and servers. It is not necessary to enable DHCP Relay if DHCP traffic is bridged through one network (the clients and servers are on the same physical network).

This chapter includes a description of DHCP Relay commands that are used to define the IP address of DHCP servers, maximum number of hops, and forward delay time. Configure DHCP Relay on the switch where routing of BOOTP/DHCP packets occur. These CLI commands are applicable for all VRF instances.

MIB information for DHCP Relay commands is as follows:

**Filename:** ALCATEL-IND1-UDP-RELAY-MIB.mib

**Module:** alcatelIND1UDPRelayMIB

A summary of the available commands is listed here.

<table>
<thead>
<tr>
<th>IP DHCP Relay</th>
<th>Generic IP UDP Relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp relay admin-state</td>
<td>ip udp relay port</td>
</tr>
<tr>
<td>ip dhcp relay destination</td>
<td>ip udp relay service</td>
</tr>
<tr>
<td>ip dhcp relay per-interface-mode</td>
<td>ip udp relay vlan</td>
</tr>
<tr>
<td>ip dhcp relay interface dest</td>
<td>ip udp relay svc</td>
</tr>
<tr>
<td>ip dhcp relay interface admin-state</td>
<td>ip udp relay address</td>
</tr>
<tr>
<td>ip dhcp relay forward-delay</td>
<td>show ip udp relay</td>
</tr>
<tr>
<td>ip dhcp relay maximum-hops</td>
<td>show ip dhcp relay statistics</td>
</tr>
<tr>
<td>ip dhcp relay insert-agent-information</td>
<td>ip dhcp relay clear statistics</td>
</tr>
<tr>
<td>ip dhcp relay insert-agent-information policy</td>
<td>show ip dhcp relay insert-agent-information error-count</td>
</tr>
<tr>
<td>ip dhcp relay insert-agent-information format</td>
<td>ip dhcp relay clear insert-agent-information error-count</td>
</tr>
<tr>
<td>ip dhcp relay pxe-support</td>
<td>show ip dhcp relay counters</td>
</tr>
<tr>
<td>show ip dhcp relay interface</td>
<td></td>
</tr>
<tr>
<td>show ip dhcp relay statistics</td>
<td></td>
</tr>
<tr>
<td>ip dhcp relay clear statistics</td>
<td></td>
</tr>
<tr>
<td>show ip dhcp relay insert-agent-information error-count</td>
<td></td>
</tr>
<tr>
<td>show ip dhcp relay clear insert-agent-information error-count</td>
<td></td>
</tr>
<tr>
<td>show ip dhcp relay counters</td>
<td></td>
</tr>
<tr>
<td>ipv6 udp relay clear statistics</td>
<td></td>
</tr>
</tbody>
</table>
### DHCP Relay Commands

<table>
<thead>
<tr>
<th>Generic IPv6 UDP Relay</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 udp relay port</td>
</tr>
<tr>
<td></td>
<td>ipv6 udp relay service</td>
</tr>
<tr>
<td></td>
<td>ipv6 udp relay vlan</td>
</tr>
<tr>
<td></td>
<td>ipv6 udp relay svc</td>
</tr>
<tr>
<td></td>
<td>ipv6 udp relay address</td>
</tr>
<tr>
<td></td>
<td>show ipv6 udp relay</td>
</tr>
<tr>
<td></td>
<td>show ipv6 udp relay statistics</td>
</tr>
<tr>
<td></td>
<td>ipv6 udp relay clear statistics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IPv6 DHCP Relay</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 dhcp relay admin-state</td>
</tr>
<tr>
<td></td>
<td>ipv6 dhcp relay interface admin-state</td>
</tr>
<tr>
<td></td>
<td>ipv6 dhcp relay destination</td>
</tr>
<tr>
<td></td>
<td>ipv6 dhcp relay maximum-hops</td>
</tr>
<tr>
<td></td>
<td>show ipv6 dhcp relay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DHCP Server Commands</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dhcp-server</td>
</tr>
<tr>
<td></td>
<td>dhcp-server restart</td>
</tr>
<tr>
<td></td>
<td>show dhcp-server leases</td>
</tr>
<tr>
<td></td>
<td>show dhcp-server statistics</td>
</tr>
<tr>
<td></td>
<td>clear dhcp-server statistics</td>
</tr>
<tr>
<td></td>
<td>dhcpv6-server</td>
</tr>
<tr>
<td></td>
<td>dhcpv6-server restart</td>
</tr>
<tr>
<td></td>
<td>show dhcpv6-server leases</td>
</tr>
<tr>
<td></td>
<td>clear dhcpv6-server statistics</td>
</tr>
<tr>
<td></td>
<td>show dhcpv6-server statistics</td>
</tr>
<tr>
<td></td>
<td>dhcp-message-service</td>
</tr>
<tr>
<td></td>
<td>dhcp-message-service restart</td>
</tr>
<tr>
<td></td>
<td>show message-service status</td>
</tr>
<tr>
<td></td>
<td>active-lease-service</td>
</tr>
<tr>
<td></td>
<td>active-lease-service restart</td>
</tr>
<tr>
<td></td>
<td>show active-lease-service status</td>
</tr>
</tbody>
</table>
### DHCP Snooping

- `dhcp-snooping admin-state`
- `dhcp-snooping mac-address-verification`
- `dhcp-snooping option-82-data-insertion`
- `dhcp-snooping bypass option-82-check`
- `dhcp-snooping option-82 format`
- `dhcp-snooping option-82 policy`
- `dhcp-snooping vlan`
- `dhcp-snooping port`
- `dhcp-snooping linkagg`
- `dhcp-snooping ip-source-filter admin-state`
- `dhcp-snooping ip-source-filter`
- `dhcp-snooping binding admin-state`
- `dhcp-snooping binding timeout`
- `dhcp-snooping binding action`
- `dhcp-snooping binding persistency`
- `dhcp-snooping binding`
- `show dhcp-snooping`
- `show dhcp-snooping ip-source-filter`
- `show dhcp-snooping vlan`
- `show dhcp-snooping port`
- `dhcp-snooping clear violation-counters`
- `show dhcp-snooping counters`
- `dhcp-snooping clear counters`
- `show dhcp-snooping isf-statistics`
- `dhcp-snooping clear isf-statistics`
- `show dhcp-snooping binding`

### DHCPv6 Snooping

- `dhcpv6-snooping vlan admin-state`
- `dhcpv6-snooping global admin-state`
- `dhcpv6-snooping binding timeout`
- `dhcpv6-snooping binding action`
- `dhcpv6-snooping binding persistency`
- `dhcpv6-snooping ipv6-source-filter`
- `ipv6 dhcp guard`
- `ipv6 dhcp guard trusted`
- `show dhcpv6-snooping`
- `show dhcpv6-snooping interfaces`
- `show dhcpv6-snooping binding`
- `show dhcpv6-snooping ipv6-source-filter`
- `show ipv6 dhcp guard`
ip dhcp relay admin-state

Enables or disables DHCP Relay for the switch for both the VLAN and Shortest Path Bridging (SPB) service domains. When enabled, DHCP packets can be relayed between a client and a server across VLANs or an SPB service domain.

**ip dhcp relay admin-state {enable | disable}**

<table>
<thead>
<tr>
<th>Syntax Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
</tr>
</tbody>
</table>

**Defaults**

By default, DHCP Relay is disabled for the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
</tr>
<tr>
<td>6465</td>
</tr>
<tr>
<td>6560</td>
</tr>
<tr>
<td>6570M</td>
</tr>
<tr>
<td>6860</td>
</tr>
<tr>
<td>6860N</td>
</tr>
<tr>
<td>6865</td>
</tr>
<tr>
<td>6900</td>
</tr>
<tr>
<td>9900</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6900 V72/C32</th>
</tr>
</thead>
</table>

| Supported | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

**Usage Guidelines**

- Disabling this feature does not remove the DHCP relay agent configuration from the switch. However, the configuration is not active unless the feature is enabled using this command.

- When this feature is enabled, DHCP packets are relayed on a global basis or on a per-interface basis.
  - Global DHCP Relay requires a global destination IP address (configured through the `ip dhcp relay destination` command). All DHCP packets are forwarded by a global relay agent.
  - Per-interface DHCP Relay is disabled by default. To enable this mode and define a per-interface relay agent, use the `ip dhcp relay per-interface-mode` and `ip dhcp relay interface destination` commands. Only DHCP packets originating from the VLAN or SPB service that is associated with the specified IP interface are forwarded by the interface relay agent.
  - The global and per-interface modes are mutually exclusive.
  - The global or per-interface mode configuration is not active unless the DHCP Relay feature is enabled for the switch.

- Configure DHCP Relay on switches where packets are routed between IP networks.

- Configuring a DHCP relay agent for an IP interface that is bound to an SPB service (a service-based IP interface) is supported only on the OmniSwitch 9900.

**Examples**

- `-> ip dhcp relay admin-state enable`
-> ip dhcp relay admin-state disable

**Release History**

Release 8.5R3; command introduced.

**Related Commands**

- `ip dhcp relay destination`  
  Configures a global destination IP address.
- `ip dhcp relay per-interface-mode`  
  Enables or disables the per-interface DHCP relay mode, which is used to process DHCP packets on a per-interface basis.
- `show ip dhcp relay interface`  
  Displays the DHCP Relay configuration.

**MIB Objects**

- `alaDhcpRelayGlobalConfig`
- `alaDhcpRelayAdminStatus`
**ip dhcp relay destination**

Configures a global destination IP address. When the global DHCP Relay mode is active, all DHCP client requests are forwarded to the specified destination IP address.

`ip dhcp relay destination ip_address`

`no ip dhcp relay destination ip_address`

**Syntax Definitions**

`ip_address` The IPv4 address (for example 21.0.0.10) of the DHCP server to which packets are relayed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove the configured DHCP relay destination.
- Configuring a global destination IP address is required when the global DHCP Relay mode is enabled for the switch.

**Examples**

- `ip dhcp relay destination 3.3.0.2`
- `ip dhcp relay destination 4.4.0.2`
- `no ip dhcp relay destination 3.3.0.2`

**Release History**

Release 8.5R3; command introduced.
Related Commands

- `ip dhcp relay admin-state`  Configures the status of the DHCP Relay feature.
- `show ip dhcp relay interface`  Displays the DHCP Relay configuration.

MIB Objects

alaDhcpRelayServerDestinationTable
  - alaDhcpRelayServerDestinationAddressType
  - alaDhcpRelayServerDestinationAddress
  - alaDhcpRelayServerDestinationRowStatus
ip dhcp relay per-interface-mode

Enables or disables the DHCP Relay per-interface mode. When this mode is enabled, a relay agent can be configured for a specific IP interface.

ip dhcp relay per-interface-mode
no ip dhcp relay per-interface-mode

Syntax Definitions
N/A

Defaults
By default, the global DHCP Relay mode is active when the DHCP Relay feature is enabled.

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
- When the per-interface DHCP relay mode is enabled with this command, the global DHCP relay mode is not available. These two types of relay agents are mutually exclusive.
- Use the no form of this command to change the DHCP Relay mode back to global (the default).
- When the per-interface mode is active, use the ip dhcp relay interface destination command to configure a destination IP address for each IP interface that will serve as a DHCP relay agent.
- The global or per-interface mode configuration is not active unless the DHCP Relay feature is enabled for the switch.

Examples
- -> ip dhcp relay per-interface-mode
- -> no ip dhcp relay per-interface-mode

Release History
Release 8.5R3; command introduced.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip dhcp relay interface destination</code></td>
<td>Configures the DHCP relay destination address for the specified IP interface.</td>
</tr>
<tr>
<td><code>ip dhcp relay interface admin-state</code></td>
<td>Enables or disables the per-interface DHCP relay agent.</td>
</tr>
<tr>
<td><code>ip dhcp relay admin-state</code></td>
<td>Enables or disables the DHCP relay feature.</td>
</tr>
<tr>
<td><code>show ip dhcp relay interface</code></td>
<td>Displays the DHCP Relay configuration.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- `alaDhcpRelayGlobalConfig`
- `alaDhcpRelayPerInterfaceMode`
ip dhcp relay interface destination

Configures a DHCP relay destination IP address for the specified interface. The specified IP interface is bound to a VLAN or an SPB service; packets destined for the specified IP address are relayed over the VLAN or SPB service domain.

```
ip dhcp relay interface if_name destination ip_address
no ip dhcp relay interface if_name destination ip_address
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_name</td>
<td>The name of an IPv4 interface on which a destination IP address is configured. Specify the primary IP interface for the VLAN or service.</td>
</tr>
<tr>
<td>ip_address</td>
<td>The Pv4 address (for example 21.0.0.10) of the DHCP server to which packets are relayed.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>---------------------------------------------</td>
<td></td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- Use the no form of this command to remove the configured DHCP relay destination for the specified interface.
- This command works only if the per-interface DHCP mode is active. Use the ip dhcp relay per-interface-mode command to enable this option.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- The IP interface must be defined for a VLAN or an SPB service before using this command. Packets destined for the specified IP address are relayed over the VLAN or SPB service domain.
- Configuring a DHCP relay agent for an IP interface that is bound to an SPB service (a service-based IP interface) is supported only on the OmniSwitch 9900.

**Examples**

```
-> ip dhcp relay interface client_traffic destination 75.0.0.10
-> ip dhcp relay interface client_traffic destination 31.0.0.20
-> no ip dhcp relay interface client_traffic destination 31.0.0.20
```
**Release History**

Release 8.5R3; command introduced.

**Related Commands**

- `ip dhcp relay per-interface-mode` Enables or disables the DHCP Relay per-interface mode.
- `ip dhcp relay interface admin-state` Enables or disables DHCP relay on an IP interface.
- `show ip dhcp relay interface` Displays the DHCP Relay configuration.

**MIB Objects**

```
dhcpRelayInterfaceTable
  dhcpRelayInterfaceName
  dhcpRelayInterfaceIpAddressType
  dhcpRelayInterfaceIpAddress
  dhcpRelayInterfaceStatus
```
ip dhcp relay interface admin-state

Enables or disables the relay of DHCP packets received on the specified interface.

```
ip dhcp relay interface if_name admin-state {enable | disable}
```

**Syntax Definitions**

- **if_name**: The name of an IPv4 interface.
- **enable**: Enables the relay of DHCP packets on the interface.
- **disable**: Disables the relay of DHCP packets on the interface.

**Defaults**

By default, DHCP relay is enabled for the interface when a relay destination IP address is configured for the interface.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

At least one relay destination must be configured before the DHCP relay is enabled for an interface.

**Examples**

```
-> ip dhcp relay interface client_traffic admin-state enable
-> ip dhcp relay interface client-traffic admin-state disable
```

**Release History**

Release 8.5R3; command introduced.
**Related Commands**

- `ip dhcp relay per-interface-mode` Enables or disables the DHCP Relay per-interface mode.
- `ip dhcp relay interface destination` Configures the DHCP relay destination address for the specified IP interface.
- `show ip dhcp relay interface` Displays the DHCP Relay configuration.

**MIB Objects**

- `alaDhcpRelayInterfaceAdminStateTable`  
- `alaDhcpRelayInterfaceAdminStatus`
ip dhcp relay forward-delay

Sets the forward delay time value for the DHCP Relay configuration. The BOOTP/DHCP packet sent from the client contains the elapsed boot time. This is the amount of time, in seconds, since the client last booted. DHCP Relay does not process the packet unless the elapsed boot time value of the client is equal to or greater than the configured value of the forward delay time.

`ip dhcp relay forward-delay seconds`

**Syntax Definitions**

*seconds*  
Forward delay time value in seconds.

**Defaults**

By default, the forward delay time is set to 0 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The time specified applies to all defined DHCP Relay agent IP addresses.
- If a packet contains an elapsed boot time value that is less than the specified forward delay time value, DHCP Relay discards the packet.

**Examples**

```bash
-> ip dhcp relay forward-delay 300
-> ip dhcp relay forward-delay 120
```

**Release History**

Release 7.1.1; command introduced.
Release 8.6R1; `ip helper forward-delay` changed to `ip dhcp relay forward-delay`. 
Related Commands

- `ip dhcp relay admin-state` Enables or disables the DHCP Relay feature for the switch.
- `ip dhcp relay maximum-hops` Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.
- `show ip dhcp relay interface` Displays current DHCP Relay configuration information.
- `show ip dhcp relay statistics` Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

- `alaDhcpRelayGlobalConfig`
  - `alaDhcpRelayForwardDelay`
ip dhcp relay maximum-hops

Sets the maximum number of hops value for the DHCP Relay configuration. This value specifies the maximum number of relays a BOOTP/DHCP packet is allowed to traverse until it reaches its server destination. Limiting the number of hops that can forward a packet prevents packets from looping through the network.

```
ip dhcp relay maximum-hops hops
```

**Syntax Definitions**

- **hops**: The maximum number of relays.

**Defaults**

By default, the maximum hops value is set to 16 hops.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a packet contains a hop count equal to or greater than the `hops` value, DHCP Relay discards the packet.
- The maximum hops value only applies to DHCP Relay and is ignored by other services.

**Examples**

```
-> ip dhcp relay maximum-hops 1
-> ip dhcp relay maximum-hops 10
```

**Release History**

Release 7.1.1; command introduced.
Release 8.6R1; *ip helper maximum-hops* changed to *ip dhcp relay maximum-hops*
Related Commands

- **ip dhcp relay admin-state**: Enables or disables the DHCP Relay feature for the switch.
- **ip dhcp relay forward-delay**: Sets the forward delay time value. DHCP Relay does not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.
- **show ip dhcp relay interface**: Displays current DHCP Relay configuration information.
- **show ip dhcp relay statistics**: Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

- `alaDhcpRelayGlobalConfig`
- `alaDhcpRelayMaximumHops`
**ip dhcp relay insert-agent-information**

Enables or disables the DHCP relay agent information option (Option-82) feature. When this feature is enabled, local relay agent information is inserted into client DHCP packets when the agent forwards these packets to a DHCP server.

```
ip dhcp relay insert-agent-information
no ip dhcp relay insert-agent-information
```

### Syntax Definitions

N/A

### Defaults

By default, this feature is disabled on the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to disable the DHCP Option-82 feature.
- This command enables the DHCP Option-82 feature for the entire switch; it is not configurable on a per-interface basis.
- When the relay agent receives a DHCP packet that already contains the Option-82 field, the packet is processed based on the agent information policy configured for the switch. This policy is configured using the `ip dhcp relay insert-agent-information policy` command.
- The DHCP Relay agent information option and DHCP Snooping are mutually exclusive. If the DHCP Relay Option-82 feature is enabled for the switch, then DHCP Snooping is not available. The reverse is also true; if DHCP Snooping is enabled, then DHCP Relay Option-82 is not available.

### Examples

```
-> ip dhcp relay insert-agent-information
-> no ip dhcp relay insert-agent-information
```

### Release History

Release 7.1.1; command introduced.
Release 8.6R1; `ip helper agent-information` changed to `ip dhcp relay insert-agent-information`. 
DHCP Relay Commands

**Related Commands**

- `ip dhcp relay insert-agent-information policy`: Configures a policy to determine how the relay agent handles DHCP packets that already contain the Option-82 field.
- `ip dhcp relay insert-agent-information format`: Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.
- `show ip dhcp relay interface`: Displays current DHCP Relay configuration information.
- `show ip dhcp relay statistics`: Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

**MIB Objects**

- `alaDhcpRelayGlobalConfig`
  
- `alaDhcpRelayInsertAgentInformation`
ip dhcp relay insert-agent-information policy

Configures a policy that determines how the DHCP relay agent handles the DHCP packets that already contain an Option-82 field.

ip dhcp relay insert-agent-information policy {drop | keep | replace}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Drop DHCP packets that already contain an Option-82 field.</td>
</tr>
<tr>
<td>keep</td>
<td>Keep the existing Option-82 field information and continue to relay the DHCP packet.</td>
</tr>
<tr>
<td>replace</td>
<td>Replace the existing Option-82 field information with local relay agent information and continue to relay the DHCP packet.</td>
</tr>
</tbody>
</table>

Defaults

By default, DHCP packets that already contain an Option-82 field are dropped.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The agent information policy is not applied if the DHCP relay agent receives a DHCP packet from a client that contains a non-zero value for the gateway IP address (giaddr). In this case, the agent does not insert the relay agent information option into the DHCP packet and forwards the packet to the DHCP server.
- Note that if a DHCP packet contains a gateway IP address (giaddr) value that matches a local subnet and also contains the Option-82 field, the packet is dropped by the relay agent.

Examples

- ip dhcp relay insert-agent-information policy drop
- ip dhcp relay insert-agent-information policy keep
- ip dhcp relay insert-agent-information policy replace

Release History

Release 7.1.1; command introduced.
Release 8.6R1; ip helper agent-information policy changed to ip dhcp relay insert-agent-information policy.
**Related Commands**

- **ip dhcp relay insert-agent-information**
  Enables the insertion of relay agent information Option-82 into DHCP packets.

- **show ip dhcp relay interface**
  Displays current DHCP Relay configuration information.

- **show ip dhcp relay statistics**
  Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

**MIB Objects**

- alaDhcpRelayGlobalConfig
- alaDhcpRelayInsertAgentInformationPolicy
ip dhcp relay insert-agent-information format

Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.

```
ip dhcp relay insert-agent-information format {base-mac | system-name | user-string string | interface-alias | auto-interface-alias | ascii {{circuit-id | remoted-id} {base-mac | cvlan | interface | interface-alias | system-name | user-string string | vlan}} {delimiter string}}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-mac</td>
<td>The base MAC address of the switch.</td>
</tr>
<tr>
<td>system-name</td>
<td>The system name of the switch.</td>
</tr>
<tr>
<td>string</td>
<td>A user defined text string. Supports up to 64 characters.</td>
</tr>
<tr>
<td>interface-alias</td>
<td>The alias configured for the interface.</td>
</tr>
<tr>
<td>auto-interface-alias</td>
<td>The switch automatically generates the interface-alias in the following format: SystemName_slot_port.</td>
</tr>
<tr>
<td>ascii</td>
<td>ASCII format. base-mac: The base MAC address of the switch. cvlan: The Customer VLAN ID. interface: The interface name. interface-alias: The alias configured for the interface. system-name: The system name of the switch. user-string: A user defined text string. vlan: The VLAN ID of which the client is a member. string: A user-defined text string. delimiter: The delimiter character that separates fields within the Circuit ID and Remote ID ASCII string value. Valid characters are</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-mac</td>
<td>base-mac</td>
</tr>
<tr>
<td>system-name</td>
<td></td>
</tr>
<tr>
<td>user-string</td>
<td></td>
</tr>
<tr>
<td>interface-alias</td>
<td></td>
</tr>
<tr>
<td>auto-interface-alias</td>
<td></td>
</tr>
<tr>
<td>ascii</td>
<td>base-mac</td>
</tr>
</tbody>
</table>
### Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines
- The string parameter specifies user-defined information to insert into the Circuit ID and Remote ID fields.
- When entering a *string* for user-defined Option-82 information, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the *string* “Building B Server” requires quotes because of the spaces between the words.
- The *interface-alias* parameter will use the alias configured with the *interfaces alias* command. If no alias is configured a NULL string will be inserted.
- A maximum of 63 characters can be inserted when using the *interface-alias* and *auto-interface-alias* parameters, remaining characters will be truncated.
- The Option-82 format option is a global setting, the format specified is applied to all ports on the switch.
- The data specified with this command is added to the Circuit ID and Remote ID fields only when DHCP Option-82 data insertion is enabled for the switch.
- The ASCII option is used to specify the type of information that is configured in ASCII text string format and then inserted into the Option-82 Circuit ID suboption. Each parameter provided with this command represents a different type of information.
  - Configuring the Circuit ID or Remote ID suboption in ASCII format allows up to five fields (types) of information within the ASCII string. However, if the contents of all the fields combined exceeds 127 characters, then the ASCII string is truncated.
  - Specifying at least one parameter with ASCII option is required. If multiple parameters are selected, then specifying one of the valid delimiter characters is also required.
  - To ensure that the “\” (backward slash) delimiter is parsed correctly, enter two backward slashes in quotes (for example, “\\”).

### Examples
- `ip dhcp relay insert-agent-information format user-string “Building B Server”`
- `ip dhcp relay insert-agent-information format system-name`
- `ip dhcp relay insert-agent-information format base-mac`
- `ip dhcp relay insert-agent-information format interface-alias`
- `ip dhcp relay insert-agent-information format auto-interface-alias`
- `ip dhcp relay insert-agent-information format ascii circuit-id user-string “Bldg A Server”`
- `ip dhcp relay insert-agent-information format ascii remote-id vlan system-name delimiter |`
- `ip dhcp relay insert-agent-information ascii interface system-name delimiter “\\”`
**Release History**

Release 8.1.1; command introduced.
Release 8.6R1; **ip helper option-82 format** changed to **ip dhcp relay insert-agent-information format**, **circuit-id** and **remote-id** parameter options added.

**Related Commands**

- **show ip dhcp relay interface**    Displays the current DHCP configuration for the switch.

**MIB Objects**

- alaDhcpRelayGlobalConfig
- alaDhcpRelayOption82FormatType
- alaDhcpRelayOption82FormatASCIIConfTable
  - alaDhcpRelayOption82FormatASCIIConfField1
  - alaDhcpRelayOption82FormatASCIIConfField2
  - alaDhcpRelayOption82FormatASCIIConfField3
  - alaDhcpRelayOption82FormatASCIIConfField4
  - alaDhcpRelayOption82FormatASCIIConfField5
  - alaDhcpRelayOption82FormatASCIIConfDelimiter
  - alaDhcpRelayOption82FormatASCIIConfStatus
ip dhcp relay pxe-support

Enables or disables relay agent support for Preboot Execution Environment (PXE) devices.

**ip dhcp relay pxe-support**

**no dhcp relay pxe-support**

### Syntax Definitions

N/A

### Defaults

By default, PXE support is disabled for the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `no` form of the command to disable PXE support.

### Examples

```
-> ip dhcp relay pxe-support
-> no ip dhcp relay pxe-support
```

### Release History

Release 7.1.1; command introduced.
Release 8.6R1; `ip helper pxe-support` changed to `ip dhcp relay pxe-support`.

### Related Commands

- **show ip dhcp relay interface** Displays current DHCP Relay configuration information.

### MIB Objects

- `alaDhcpRelayGlobalConfig`
- `alaDhcpRelayPxeSupport`
**show ip dhcp relay interface**

Display the DHCP Relay and Relay Agent information.

```
show ip dhcp relay interface
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8</th>
<th>C32E/T24C2</th>
<th>X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- DHCP packets are relayed on a global basis or on a per-interface basis.

- When the global DHCP Relay mode is active (the default), a global destination IP address is required. Global destination IP addresses are displayed in the **Relay Destination list** field.

- When the per-interface DHCP Relay mode is enabled, destination IP addresses are configured for specific interfaces. The **Relay Destination list** displays these IP addresses along with the name of the IP interface associated with each address.

**Examples**

```
-> show ip dhcp relay interface
IP DHCP Relay:
  DHCP Relay Admin Status = Disable,
  Forward Delay(seconds)  = 0,
  Max number of hops      = 16,
  Relay Agent Information = Disabled,
  Relay Agent Information Policy = Drop,
  DHCP Relay Opt82 Format = Base MAC,
  DHCP Relay Opt82 String = 00:e0:b1:e7:09:a3,
  PXE support             = Disabled,
  Relay Mode              = Global,
  Bootup Option           = Disable,
  Relay Destination list (Global Mode):
    From Interface Any to Server 128.100.16.1

-> show ip dhcp relay interface
```
IP DHCP Relay:
- DHCP Relay Admin Status = Enable,
- Forward Delay (seconds) = 0,
- Max number of hops = 16,
- Relay Agent Information = Disabled,
- Relay Agent Information Policy = Drop,
- DHCP Relay Opt82 Format = Base MAC,
- DHCP Relay Opt82 String = 2c:fa:a2:13:e4:02,
- PXE support = Disabled,
- Relay Mode = Per Interface,
- Bootup Option = Disable,
- Relay Destination list (Per Interface Mode):
  - From Interface ipvpl to Server 50.3.3.1

Output definitions

**DHCP Relay Admin Status**
The status (Enable or Disable) of DHCP Relay. Configured through the `ip dhcp relay admin-state` command.

**Forward Delay (seconds)**
The current forward delay time. Use the `ip dhcp relay forward-delay` command to change this value.

**Max number of hops**
The current maximum number of hops allowed. Use the `ip dhcp relay maximum-hops` command to change this value.

**Relay Agent Information**
Indicates whether the DHCP relay agent information option (Option-82) is Enabled or Disabled. Configured through the `ip dhcp relay insert-agent-information` command.

**Relay Agent Information Policy**
The policy configured to determine how the DHCP relay agent handles the DHCP packets that already contain an Option-82 field. Configured through the `ip dhcp relay insert-agent-information policy` command.

**DHCP Relay Opt82 Format**
The type of Option-82 information inserted. Configured through the `ip dhcp relay insert-agent-information format` command.

**DHCP Relay Opt82 String**
The Option-82 string based on the specified Option-82 format.

**PXE support**
Specifies the status (Enabled or Disabled) of the relay agent support for PXE devices. By default the PXE support is disabled. Configured through the `ip dhcp relay pxe-support` command.

**Relay Mode**
Whether DHCP Relay is set to operate in the global mode or the per-interface mode. Configured through the `ip dhcp relay per-interface-mode` command.

**Bootup Option**
Indicates whether or not automatic IP address configuration for a specific VLAN is done when the switch boots up (Enabled or Disabled). Configured through the `ip interface dhcp-client` command.

**Relay Destination list**
IP addresses for DHCP servers that receive BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the `ip dhcp relay destination` command (global mode) or `ip dhcp relay interface destination` (per-interface mode) to add or remove DHCP server IP addresses from the DHCP Relay configuration.

**Release History**
- Release 8.5R3; command introduced.
- Release 8.6R1; “Relay Agent Information” field added.
Related Commands

show ip dhcp relay statistics  Displays the collected DHCP Relay statistics.

MIB Objects

N/A
**show ip dhcp relay statistics**

Displays all DHCP Relay statistics collected.

**show ip dhcp relay statistics**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The following DHCP Relay statistics are collected:
  - The number of packets DHCP Relay has received.
  - The number of packets dropped due to forward delay, maximum hops, relay agent, and gateway IP violations.
  - Statistics that apply to a specific DHCP server (such as the number of packets transmitted to the server and the number of invalid Option-82 DHCP server packets dropped by the relay agent).
  - The number of packets processed since the last time these statistics were displayed.

- Use the `ip dhcp relay clear statistics` command to clear all DHCP Relay statistics.

**Examples**

```
-> show ip dhcp relay statistics
Global Statistics :
    Reception From Client :
        Total Count = 12, Delta = 12
    Forw Delay Violation :
        Total Count = 3, Delta = 3
    Max Hops Violation :
        Total Count = 0, Delta = 0
    Agent Info Violation :
        Total Count = 0, Delta = 0
    Invalid Gateway IP :
        Total Count = 0, Delta = 0
Server Specific Statistics :
    From Interface ipv4-v200 to Server 75.0.0.1
```
DHCP Relay Commands

show ip dhcp relay statistics

Tx Server:
  Total Count = 9, Delta = 9
InvAgentInfoFromServer:
  Total Count = 0, Delta = 0

Output definitions

<table>
<thead>
<tr>
<th>Reception From Client</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forw Delay Violation</td>
<td>Number of packets dropped as a result of forward delay violations. A violation occurs if a client packet contains an elapsed boot time value that is less than the configured DHCP Relay forward delay time value.</td>
</tr>
<tr>
<td>Max Hops Violation</td>
<td>Number of packets dropped as a result of maximum hop violations. A violation occurs if a packet contains a hop count equal to or greater than the configured DHCP Relay maximum hops value.</td>
</tr>
<tr>
<td>Agent Info Violation</td>
<td>Number of packets dropped as a result of a relay agent information (Option-82) violation. A violation occurs if an Option-82 DHCP packet contains a zero gateway IP address (giaddr) and the relay agent information policy is set to <strong>Drop</strong> or a DHCP packet has no Option-82 field and contains a non-zero giaddr.</td>
</tr>
<tr>
<td>Invalid Gateway IP</td>
<td>Number of packets dropped as a result of a gateway IP violation. A violation occurs if an Option-82 DHCP packet contains a gateway IP address (giaddr) that matches a local subnet address.</td>
</tr>
</tbody>
</table>

**Delta**

Total number of packets processed since the last time the DHCP Relay statistics were checked during any user session.

**Server**

DHCP server IP address that receives BOOTP/DHCP packets forwarded by this DHCP Relay service.

**Tx Server**

Number of packets DHCP Relay has transmitted to the DHCP server.

**InvAgentInfoFromServer**

Number of invalid Option-82 DHCP server packets dropped by the relay agent.

**Delta**

The difference between the number of packets received from the client and the number of packets transmitted to the DHCP server since the last time DHCP Relay statistics were checked during any user session.

Release History

Release 8.5R3; command introduced.

Related Commands

- **ip dhcp relay admin-state**
  Enables or disables the DHCP relay feature.
- **ip dhcp relay clear statistics**
  Resets the DHCP Relay statistic counters to zero.
- **show ip dhcp relay insert-agent-information error-count**
  Displays the Option-82 related error statistics.

MIB Objects

N/A
**ip dhcp relay clear statistics**

Clears DHCP relay statistics collected.

```
ip dhcp relay clear statistics [global-only | destination ip_address | interface if_name destination ip_address]
```

### Syntax Definitions

- **global-only**
  - Clears statistics collected for global DHCP Relay.
- **ip_address**
  - The IPv4 destination address for which statistics are cleared.
- **if_name**
  - The IPv4 interface name for which statistics are cleared.

### Defaults

By default, all DHCP Relay statistics are cleared.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When this command is used, all DHCP Relay statistics are reset to zero.
- Use the `show ip dhcp relay statistics` command to display DHCP Relay statistics.

### Examples

- `-> ip dhcp relay clear statistics`
- `-> ip dhcp relay clear statistics global-only`
- `-> ip dhcp relay clear statistics destination 75.0.0.2`
- `-> ip dhcp relay clear statistics interface ipv4-200 destination 75.0.0.2`

### Release History

Release 8.5R3; command introduced.
Release 8.6R1; `clear ip dhcp relay statistics` changed to `ip dhcp relay clear statistics` and `global-only`, `destination`, `interface` parameters added.
**Related Commands**

- `ip dhcp relay admin-state` Enables or disables the DHCP Relay feature.
- `show ip dhcp relay statistics` Displays DHCP Relay statistics.

**MIB Objects**

- `alaDhcpRelayGlobalConfig`
  - `alaDhcpRelayStatisticsClear`
- `alaDhcpRelayClearStatisticsTable`
  - `alaDhcpRelayClearStatisticsAction`
**show ip dhcp relay insert-agent-information error-count**

Displays the Option-82 related error statistics on a per-port and per-interface basis.

```
show ip dhcp relay insert-agent-information error-count [interface if_name | port chassis/slot/port [interface if_name]]
```

**Syntax Definitions**

- **if_name**
  The name of the IPv4 interface for which the Option-82 error count statistics are displayed.

- **chassis/slot/port**
  The chassis, slot, and port number of the port for which the Option-82 error count statistics are displayed.

**Defaults**

By default, all Option-82 error count statistics are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- To display the statistics for a specific port, use the **port chassis/slot/port** parameter option.
- To display the statistics for a specific IPv4 interface, use the **interface if_name** parameter option.
- Use the **ip dhcp relay clear insert-agent-information error-count** command to clear Option-82 error statistics.

**Examples**

```
-> show ip dhcp relay insert-agent-information error-count port 1/1/3
Slot/Port | Interface | Agent Info Violation | Invalid Gateway IP
-------------------------------+---------------------+---------------------
      1/1/3   ipv4-v100          500                      0
      1/1/3   ipv4-v200          0                       10
      1/1/3   ipv4-v1100         500                      0
      1/1/3   ipv4-v3100         500                      0

-> show ip dhcp relay insert-agent-information error-count interface ipv4-v100
Slot/Port | Interface | Agent Info Violation | Invalid Gateway IP
-------------------------------+---------------------+---------------------
      1/1/3   ipv4-v100         400                      0
      2/1/3   ipv4-v100         500                      0
```
-> show ip dhcp relay insert-agent-information error-count port 1/1/3 interface ipv4-v100

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Interface</th>
<th>Agent Info Violation</th>
<th>Invalid Gateway IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/3</td>
<td>ipv4-v100</td>
<td>500</td>
<td>0</td>
</tr>
</tbody>
</table>

Output definitions

<table>
<thead>
<tr>
<th>Slot/port</th>
<th>The chassis, slot, and port number for which the error count statistics is displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The name of the IPv4 interface associated with the port.</td>
</tr>
<tr>
<td>Agent Info Violation</td>
<td>Number of packets dropped as a result of a relay agent information (Option-82) violation. A violation occurs if an Option-82 DHCP packet contains a zero gateway IP address (giaddr) and the relay agent information policy is set to <strong>Drop</strong> or a DHCP packet has no Option-82 field and contains a non-zero giaddr.</td>
</tr>
<tr>
<td>Invalid Gateway IP</td>
<td>Number of packets dropped as a result of a gateway IP violation. A violation occurs if an Option-82 DHCP packet contains a gateway IP address (giaddr) that matches a local subnet address.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command introduced.
Release 8.6.R1; **show ip helper option-82 error-count** changed to **show ip dhcp relay insert-agent-information error-count** and **vlan** changed to **interface**.

Related Commands

**ip dhcp relay insert-agent-information format** Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.

**show ip dhcp relay interface** Displays current DHCP Relay configuration information.

MIB Objects

alaDhcpRelayOpt82ErrStatsTable
  - alaDhcpRelayOpt82ErrStatsIfIndex
  - alaDhcpRelayOpt82ErrStatsIfName
  - alaDhcpRelayOpt82ErrStatsAgentInfoViolation
  - alaDhcpRelayOpt82ErrStatsInvalidGatewayIPAddr
ip dhcp relay clear insert-agent-information error-count

Clears the Option-82 related error statistics on a per-port and per-interface basis.

**ip dhcp relay clear insert-agent-informaton error-count [interface if_name | port chassis/slot/port]**

### Syntax Definitions

- **if_name**: The name of the IPv4 interface for which the Option-82 error count statistics are cleared.
- **chassis/slot/port**: The chassis, slot, and port number of the port for which the Option-82 error count statistics are cleared.

### Defaults

By default, all Option-82 error count statistics are cleared.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- To clear the statistics for a specific IPv4 interface, use the **interface if_name** parameter option.
- To clear the statistics for a specific port, use the **port chassis/slot/port** parameter option.
- When this command is used, all Option-82 error statistics are reset to zero.
- Use the **show ip dhcp relay insert-agent-information error-count** command to display Option-82 statistics collected.

### Examples

- `-> ip dhcp relay clear insert-agent-information error-count`
- `-> ip dhcp relay clear insert-agent-information error-count interface ipv4-v100`
- `-> ip dhcp relay clear insert-agent-information error-count port 1/1/3`

### Release History

Release 8.6R1; command introduced.
Related Commands

- **ip dhcp relay insert-agent-information format**  
  Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.

- **show ip helper**  
  Displays current DHCP Relay configuration information.

MIB Objects

- `alaDhcpRelayOpt82ErrStatsTable`
- `alaDhcpRelayOpt82ErrStatsReset`
show ip dhcp relay counters

Displays DHCP Relay packet statistics.

show ip dhcp relay counters

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to display statistics for the various types of DHCP packets that were relayed or passed through by the switch.

Examples

-> show ip dhcp relay counters
DHCP Packets:
DHCP Discover Packets : 0,
DHCP Offer Packets    : 0,
DHCP Request Packets  : 0,
DHCP ACK Packets      : 0,
DHCP NACK Packets     : 0,
DHCP Release Packets  : 0,
DHCP Decline Packets  : 0,
DHCP Inform Packets   : 0,
DHCP Renew Packets    : 0,

Release History

Release 8.6R1; command introduced.
Related Commands

- `ip dhcp relay admin-state`  Enables or disables the DHCP relay feature.
- `show ip dhcp relay statistics`  Displays DHCP Relay error statistics.
- `show ip dhcp relay insert-agent-information error-count`  Displays the Option-82 related error statistics.

MIB Objects

N/A
ip helper address

Adds or deletes a DHCP server IP address. DHCP Relay forwards BOOTP/DHCP broadcasts to and from the specified address. If multiple DHCP servers are used, configure one IP address for each server.

```
ip helper address ip_address
no ip helper address [ip_address]
```

**Syntax Definitions**

- `ip_address` DHCP server IP address (for example 21.0.0.10).

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- Use the `no` form of this command to delete an IP address from the DHCP Relay service. If an address is not specified, then all addresses are deleted.

- Using this command enables a Global DHCP Relay service on the switch. When the DHCP Relay is specified by the DHCP server IP address, the service is called Global DHCP.

- When the DHCP Relay is specified by the VLAN number of the DHCP request, the service is referred to as Per-VLAN DHCP.

- Global DHCP and Per-VLAN DHCP are mutually exclusive. You can only configure one or the other.

- Use this command to configure DHCP Relay on switches where packets are routed between IP networks.

**Examples**

```
-> ip helper address 75.0.0.10
-> no ip helper address 31.0.0.20
```

**Release History**

- Release 7.1.1; command introduced.
- Release 8.6R1; command deprecated (use `ip dhcp relay destination`).
Related Commands

**ip helper vlan address**
Specifies or deletes DHCP Relay based on the VLAN of the DHCP request.

**ip dhcp relay forward-delay**
Sets the forward delay time value. DHCP Relay does not process a client packet unless the packet contains an elapsed boot time value that is equal to or greater than the configured value of the forward delay time.

**ip dhcp relay maximum-hops**
Sets the maximum number of hops value to specify how many relays a BOOTP/DHCP packet can traverse.

**show ip helper**
Displays current DHCP Relay configuration information.

**show ip helper statistics**
Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

MIB Objects

- **iphelperTable**
- **iphelperService**
- **iphelperForwAddr**
**ip helper vlan address**

Configures a DHCP Relay service for the specified VLAN. This command is used when a per-VLAN only relay service is active on the switch. It does not apply when a standard relay service is used.

```
ip helper vlan vlan_id[-vlan_id2] address ip_address
no ip helper vlan vlan_id[-vlan_id2] address ip_address
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id[-vlan_id2]</td>
<td>VLAN ID number of the DHCP server VLAN. Use a hyphen to specify a range of VLAN IDs (3-5).</td>
</tr>
<tr>
<td>ip_address</td>
<td>IP address (for example 21.0.0.10) of the DHCP server VLAN.</td>
</tr>
</tbody>
</table>

**Defaults**

If no VLAN identification number is entered, VLAN ID 0 is used by default.

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- Specifying multiple VLAN IDs and/or a range of VLAN IDs on the same command line is allowed. Use a hyphen to indicate a contiguous range of VLAN ID entries. (for example, 10-15).
- The `ip helper vlan address` command works only if the `per-vlan-only` forwarding option is active. Use the `ip helper per-vlan-only` command to enable this option.
- Configure DHCP Relay on switches where packets are routed between IP networks.
- The IP interface must be defined for the VLANs before using this command.
- Use the `no` form of this command to delete the DHCP server VLAN from the DHCP Relay.

**Examples**

```
-> ip helper vlan 3 address 75.0.0.10
-> ip helper vlan 250-255 address 198.206.15.2
-> no ip helper vlan 3 address 75.0.0.1
-> no ip helper vlan 1601 address 198.206.15.20
```

**Release History**

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use `ip dhcp relay interface destination`).
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip helper per-vlan-only</td>
<td>Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN.</td>
</tr>
<tr>
<td>show ip helper</td>
<td>Displays current DHCP Relay configuration information.</td>
</tr>
<tr>
<td>show ip helper statistics</td>
<td>Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.</td>
</tr>
</tbody>
</table>

### MIB Objects

```
iphelperTable
    iphelperService
    iphelperVlan
```
**ip helper standard**

Sets the DHCP Relay forwarding option to standard. All DHCP packets are processed by a global relay service.

```
ip helper standard
```

### Syntax Definitions

N/A

### Defaults

By default, the DHCP Relay forwarding option is set to **standard**.

### Platforms Supported

Not supported in this release.

### Usage Guidelines

To process DHCP packets on a per VLAN basis or to change the DHCP Relay forwarding option from standard to per VLAN, use the `ip helper per-vlan-only` command.

### Examples

```
-> ip helper standard
```

### Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use the no form of the `ip dhcp relay per-interface-mode`).

### Related Commands

- `show ip helper` Displays current DHCP Relay configuration information.
- `show ip helper statistics` Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

### MIB Objects

- `iphelperStatTable`
- `iphelperForwOption`
ip helper per-vlan-only

Sets the DHCP Relay forwarding option to process only DHCP packets received from a specific, identified VLAN. This option allows each VLAN to have its own relay.

Syntax Definitions
N/A

Defaults
By default, the UDP forwarding option is set to standard.

Platforms Supported
Not supported in this release.

Usage Guidelines

- When the forwarding option is set to per-vlan-only, the standard (global) DHCP relay service is not available. These two types of services are mutually exclusive.

- To process DHCP packets on a per VLAN basis, or to change the DHCP Relay forwarding option from standard to per VLAN, use the ip helper per-vlan-only command.

- Using the per-vlan-only forwarding option requires you to specify a DHCP server IP address for each VLAN that provides a relay service. The ip helper vlan address command performs this function and at the same time enables relay for the specified VLAN.

Examples
-> ip helper per-vlan-only

Release History
Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use ip dhcp relay per-interface-mode).
**Related Commands**

- **ip helper vlan address**
  Configures a DHCP Relay service for the specified VLAN.

- **ip helper standard**
  Sets DHCP Relay forwarding option to standard. All DHCP packets are processed.

- **show ip helper**
  Displays current DHCP Relay configuration information.

- **show ip helper statistics**
  Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

**MIB Objects**

- **iphelperStatTable**
  - **iphelperForwOption**
show ip helper

Displays the current DHCP Relay and Relay Agent Information.

show ip helper

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

Displays information for all IP addresses configured.

**Examples**

```bash
-> show ip helper
Ip helper :
     Forward Delay(seconds) = 300,
     Max number of hops = 5,
     Relay Agent Information = Enabled,
     Relay Agent Information Policy = Keep,
     DHCP Opt82 Format = Base MAC,
     DHCP Opt82 String = 2c:fa:a2:13:e4:02,
     PXE support = Enabled,
     Forward option = standard mode,
     Bootup Option = Disable,
     Bootup Packet Option = DHCP
     Forwarding address list (Standard mode):
     128.100.16.1
```

**output definitions**

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Delay</td>
<td>The current forward delay time (default is three seconds). Use the <code>ip dhcp relay forward-delay</code> command to change this value.</td>
</tr>
<tr>
<td>Max number of hops</td>
<td>The current maximum number of hops allowed (default is four hops). Use the <code>ip dhcp relay maximum-hops</code> command to change this value.</td>
</tr>
<tr>
<td>Relay Agent Information</td>
<td>Indicates the status (Enabled or Disabled) of the DHCP relay agent information option feature. Configured through the <code>ip dhcp relay insert-agent-information</code> command.</td>
</tr>
<tr>
<td>Relay Agent Information Policy</td>
<td>The policy configured to determine how the DHCP relay agent handles the DHCP packets that already contain an Option-82 field. Configured through the <code>ip dhcp relay insert-agent-information policy</code> command.</td>
</tr>
</tbody>
</table>
**DHCP Relay Commands**

### Output Definitions

- **DHCP Opt82 Format**
  The type of option-82 information inserted. Configured through the `show ip dhcp relay insert-agent-information format` command.

- **DHCP Opt82 String**
  The option-82 string based on the specified Option-82 format.

- **PXE support**
  Specifies the status (Enabled or Disabled) of the relay agent support for PXE devices. By default the PXE support is disabled. Configured through the `ip dhcp relay pxe-support` command.

- **Forward option**
  The current forwarding option setting: standard mode.

- **Bootup Option**
  Indicates whether or not automatic IP address configuration for default VLAN 1 is done when the switch boots up (Enabled or Disabled). Configured through the `ip interface dhcp-client` command.

- **Bootup Packet Option**
  Indicates if the Bootup Option broadcasts a DHCP or BOOTP packet to obtain an IP address for default VLAN 1.

- **Forwarding Addresses**
  IP addresses for DHCP servers that receive BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the `ip helper address` command to add or remove DHCP server IP addresses from the DHCP Relay configuration.

### Release History

- Release 7.1.1; command introduced.
- Release 8.6R1; command deprecated (use `show ip dhcp relay interface`)

### Related Commands

- **show ip dhcp relay statistics**
  Displays DHCP Relay statistics, including the number of client packets received and transmitted to the DHCP server and packets dropped due to forward delay time and maximum hops violations.

### MIB Objects

- iphelperTable
  - iphelperService
  - iphelperForwAddr
  - iphelperForwDelay
  - iphelperMaxHops
  - iphelperAgentInformation
  - iphelperAgentInformationPolicy
  - iphelperStatTable
    - iphelperBootupOption
    - iphelperBootupPacketOption
**show ip helper statistics**

Displays the number of packets DHCP Relay has received, the number of packets dropped due to forward delay and maximum hops violations. It also displays the number of packets processed since the last time these statistics were displayed. It includes statistics that apply to a specific DHCP server, such as the number of packets transmitted to the server and the difference between the number of packets received from a client and the number transmitted to the server.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

Use the `no ip helper statistics` command to clear DHCP Relay statistics.

**Examples**

```plaintext
-> show ip helper statistics

Global Statistics :
   Reception From Client :
       Total Count = 12, Delta = 12,
   Forw Delay Violation :
       Total Count = 3, Delta = 3,
   Max Hops Violation :
       Total Count = 0, Delta = 0,
   Agent Info Violation :
       Total Count = 0, Delta = 0,
   Invalid Gateway IP :
       Total Count = 0, Delta = 0,
Server Specific Statistics :
   From any Vlan to Server 5.5.5.5
   Tx Server :
       Total Count = 9, Delta = 9
   InvAgentInfoFromServer :
       Total Count = 0, Delta = 0
```

**output definitions**

<table>
<thead>
<tr>
<th>Reception From Client</th>
<th>Number of packets DHCP Relay has received from the DHCP client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forw Delay Violation</td>
<td>Number of packets dropped as a result of forward delay violations. A violation occurs if a client packet contains an elapsed boot time value that is less than the configured DHCP Relay forward delay time value.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip dhcp relay interface</td>
<td>Displays current DHCP Relay configuration information.</td>
</tr>
<tr>
<td>no ip helper statistics</td>
<td>Resets IP helper statistics.</td>
</tr>
</tbody>
</table>

### MIB Objects

```
iphelperStatTable
    iphelperServerAddress
    iphelperRxFromClient
    iphelperTxToServer
    iphelperMaxHopsViolation
    iphelperForwDelayViolation
    iphelperResetAll
```

### Release History

- Release 7.1.1; command introduced.
- Release 8.6R1; command deprecated (use `show ip dhcp relay statistics`).

### Output Definitions (continued)

<table>
<thead>
<tr>
<th>Max Hops Violation</th>
<th>Number of packets dropped as a result of maximum hop violations. A violation occurs if a packet contains a hop count equal to or greater than the configured DHCP Relay maximum hops value.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Info Violation</td>
<td>Number of packets dropped as a result of a relay agent information (Option-82) violation. A violation occurs if an Option-82 DHCP packet contains a zero gateway IP address (giaddr) and the relay agent information policy is set to <strong>Drop</strong> or a DHCP packet has no Option-82 field and contains a non-zero giaddr.</td>
</tr>
<tr>
<td>Invalid Gateway IP</td>
<td>Number of packets dropped as a result of a gateway IP violation. A violation occurs if an Option-82 DHCP packet contains a gateway IP address (giaddr) that matches a local subnet address.</td>
</tr>
<tr>
<td>Server</td>
<td>DHCP server IP address that receives BOOTP/DHCP packets forwarded by this DHCP Relay service. Use the <code>ip helper address</code> command to add or remove DHCP server IP addresses from DHCP Relay configuration.</td>
</tr>
<tr>
<td>Tx Server</td>
<td>Number of packets DHCP Relay has transmitted to the DHCP server.</td>
</tr>
<tr>
<td>Delta</td>
<td>The difference between the number of packets received from the client and the number of packets transmitted to the DHCP server since the last time DHCP Relay statistics were checked during any user session.</td>
</tr>
<tr>
<td>Invalid Agent Info From Server</td>
<td>Number of invalid Option-82 DHCP server packets dropped by the relay agent.</td>
</tr>
<tr>
<td>Delta</td>
<td>Total number of packets processed since the last time the <code>ip helper statistics</code> were checked during any user session.</td>
</tr>
</tbody>
</table>
no ip helper statistics

Resets the IP helper statistics for the specified VRF instances.

**no ip helper statistics [global-only | server-only | address ip_address | vlan vlan_id {address ip_address}]**

### Syntax Definitions

- **global-only**: Specifies that only the global IP helper statistics must be reset.
- **server-only**: Specifies that only the IP helper statistics related to the server must be reset.
- **vlan_id**: Specifies the VLAN ID for the per-VLAN mode instance.
- **ip_address**: Specifies the IP address for the flat mode instance.

### Defaults

N/A

### Platforms Supported

Not supported in this release.

### Usage Guidelines

- This command works only for VRF instances.
- To reset all the IP helper related statistics, use this command without the additional keywords.
- To reset the IP helper statistics for the flat mode instance, provide the related IP address with the `address` keyword.
- To reset the IP helper statistics for the per-vlan mode instance, provide the VLAN ID with the `vlan` keyword and the related IP address with the `address` keyword.

### Examples

- `-> no ip helper statistics`
- `-> no ip helper statistics global-only`
- `-> no ip helper statistics server-only`
- `-> no ip helper statistics address 172.6.5.1`
- `-> no ip helper statistics vlan 20 address 172.6.5.1`

### Release History

Release 7.1.1; command introduced.
Release 8.6R1; command deprecated (use `ip dhcp relay clear statistics`)
Related Commands

show ip helper statistics  Displays the current statistics for each UDP port relay service.

MIB Objects

iphelperStatsTable
  iphelperResetAllStats
  iphelperResetSrvStats
ip udp relay port

Enables or disables generic UDP relay for the specified UDP service port. A user-defined or well-known UDP port number is specified with this command.

**ip udp relay port** *port_num* [description *description*]  
ip udp relay no port *port_num*

---

**Syntax Definitions**

*port_num*  
A UDP service port number (for example, 53, 69, 301).

*description*  
An optional description for the specified UDP service port.

---

**Defaults**

By default, relay is enabled on the BOOTP/DHCP well-known ports.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to disable generic UDP relay for the specified port.
- Use the **ip dhcp relay** commands to configure functionality for BOOTP/DHCP well-known ports (67/68).

**Examples**

- `-> ip udp relay port 54`
- `-> ip udp relay port 54 description “Generic UDP Service”`
- `-> ip udp relay no port 54`
- `-> ip udp relay port 69 description “TFTP relay”`
- `-> ip udp relay no port 69`

---

**Release History**

Release 7.1.1; command introduced.
Related Commands

**ip udp relay vlan**
Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.

**ip udp relay svc**
Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded.

**ip udp relay address**
Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.

**show ip udp relay**
Displays the current configuration for UDP services by service name or by service port number.

MIB Objects

genericUdpServiceTable
- genericUdpServiceUdpPort
- genericUdpServiceDescription
- genericUdpServiceRowStatus
**ip udp relay service**

Enables or disables generic UDP relay for the specified UDP service name (NBNS, NBDD, or other well-known UDP ports).

```
ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} [description description]
ip udp relay no service {tftp | tacacs | ntp | nbns | nbdd | dns}
```

**Syntax Definitions**

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **nbns**: NBNS well-known ports 137.
- **nbdd**: NBDD well-known port 138.
- **dns**: DNS well-known port 53.
- **description**: An optional description for the specified UDP well-known service port.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>service name and port #</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to disable UDP Relay for the specified service port.
- The **description** parameter is used with any of the **service** keywords and provides a user-defined description to identify the port service.
- If port relay is enabled for the NBDD well-known port, NBNS is not automatically enabled by default.
- Note that when UDP port relay is enabled for NTP, relay cannot forward NTP packets that contain a destination IP address that matches a VLAN router IP address on the switch.

**Examples**

```
-> ip udp relay service dns
```
-> ip udp relay service dns description dns_1
-> ip udp relay no service dns

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip udp relay vlan</td>
<td>Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.</td>
</tr>
<tr>
<td>ip udp relay svc</td>
<td>Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded.</td>
</tr>
<tr>
<td>ip udp relay address</td>
<td>Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.</td>
</tr>
<tr>
<td>show ip udp relay</td>
<td>Displays the current configuration for UDP services by service name or by service port number.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- genericUdpServiceTable
  - genericUdpServiceUdpPort
  - genericUdpServiceDescription
  - genericUdpServiceRowStatus
**ip udp relay vlan**

Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.

```
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port port_num [description description]} vlan vlan_id[-vlan_id2]
```

```
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port port_num} no vlan vlan_id[-vlan_id2]
```

**Syntax Definitions**

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **nbns**: NBNS well-known ports 137.
- **nbdd**: NBDD well-known port 138.
- **dns**: DNS well-known port 53.
- **port_num**: A user-defined port number.
- **description**: A description of the UDP service.
- **vlan_id[-vlan_id2]**: VLAN ID number. Use a hyphen to specify a range of VLAN IDs (3-5).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the VLAN association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.

**Examples**

- `-> ip udp relay service DNS vlan 10`
- `-> ip udp relay service DNS vlan 500-550`
- `-> ip udp relay service DNS no vlan 10`
-> ip udp relay port 3047 vlan 20
-> ip udp relay port 3047 no vlan 20

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **ip udp relay port** Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
- **ip udp relay service** Enables or disables generic UDP relay for well-known UDP service names.
- **ip udp relay svc** Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded.
- **ip udp relay address** Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.
- **show ip udp relay** Displays the current configuration for UDP services by service name or by service port number.

**MIB Objects**

- **genericUdpServiceDstTable**
  - **genericUdpServicePort**
  - **genericUdpServiceDstVlan**
  - **genericUdpServiceDstTblRowStatus**
**ip udp relay svc**

Specifies a Shortest Path Bridging (SPB) service on which traffic destined for a UDP port is forwarded.

```
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port port_num [description description]} svc service_id[-service_id2]
```

```
ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} | port port_num} no svc service_id[-service_id2]
```

---

**Syntax Definitions**

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **nbns**: NBNS well-known ports 137.
- **nbdd**: NBDD well-known port 138.
- **dns**: DNS well-known port 53.
- **port_num**: A user-defined port number.
- **description**: A description of the UDP service.
- **service_id[-service_id2]**: SPB service ID number. Use a hyphen to specify a range of service IDs (3-5).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the SPB service association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.

**Examples**

- `-> ip udp relay service dns svc 10`
- `-> ip udp relay service dns svc 50-55`
- `-> ip udp relay service dns no svc 10`
DHCP Relay Commands

-> ip udp relay port 3047 svc 20
-> ip udp relay port 3047 no svc 20

**Release History**

Release 8.5R4; command introduced.

**Related Commands**

- **ip udp relay port**  
  Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.

- **ip udp relay service**  
  Enables or disables generic UDP relay for well-known UDP service names.

- **ip udp relay vlan**  
  Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.

- **ip udp relay address**  
  Specifies the UDP server IP address to which traffic destined for the specified UDP port is forwarded as unicast packets.

- **show ip udp relay**  
  Displays the current configuration for UDP services by service name or by service port number.

**MIB Objects**

- **alaGenericUdpServiceSvcTable**
  - **alaGenericUdpServiceSvcPort**
  - **alaGenericUdpServiceDstSvc**
  - **alaGenericUdpServiceSvcRowStatus**
**ip udp relay address**

Specifies the UDP server IP address to which traffic destined for a UDP port is forwarded as unicast packets.

```
ip udp relay {service {tftp | tacacs | ntp | nbns | nbdd | dns} | port port_num [description description]} address ip_address
```

```
ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} | port port_num} no address ip_address
```

**Syntax Definitions**

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **nbns**: NBNS well-known ports 137.
- **nbdd**: NBDD well-known port 138.
- **dns**: DNS well-known port 53.
- **port_num**: A user-defined port number.
- **description**: A description of the UDP service.
- **ip_address**: The IPv4 address of a UDP server.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Yes</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the IP address association with the UDP service port.
- The UDP port must be created before using this command.
- Only one IP address can be configured for a UDP port (multiple IP addresses for the same UDP port is not supported).
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.
• When the specified UDP port is associated with an IP address, the relay is operating at the Layer 3 level; any attempt to then assign a VLAN or SPB service to that UDP port is blocked. UDP ports associated with a VLAN or SPB service are operating at the Layer 2 level.

**Examples**

- `ip udp relay service dns address 10.2.2.1`
- `ip udp relay service tftp address 20.2.2.1`
- `ip udp relay service dns no address 10.2.2.1`
- `ip udp relay port 3047 address 10.2.2.1`
- `ip udp relay port 3047 address 10.2.2.1`

- `ip udp relay port 54 address 30.2.2.1`
- `ip udp relay port 54 vlan 200`
ERROR: UDP port configured in L3 mode

- `ip udp relay port 64 vlan 200`
- `ip udp relay port 64 address 40.2.2.1`
ERROR: UDP port configured in L2 mode

**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `ip udp relay port` Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
- `ip udp relay service` Enables or disables generic UDP relay for well-known UDP service names.
- `ip udp relay vlan` Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.
- `ip udp relay svc` Specifies the Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded.
- `show ip udp relay` Displays the current configuration for UDP services by service name or by service port number.

**MIB Objects**

- `alaGenericUdpServiceDstIpTable`
  - `alaGenericUdpServiceDstUdpPort`
  - `alaGenericUdpServiceDstIpType`
  - `alaGenericUdpServiceDstIpAddress`
  - `alaGenericUdpServiceDstIpRowStatus`
**show ip udp relay**

Displays the generic UDP relay service configuration.

```
show ip udp relay [service {tftp | tacacs | ntp | nbns | nbdd | dns} | port port_num]
```

### Syntax Definitions

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **nbns**: NBNS well-known ports 137.
- **nbdd**: NBDD well-known port 138.
- **dns**: DNS well-known port 53.
- **port_num**: A user-defined or well-known port number.

### Defaults

By default, the configuration for all UDP services is shown.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a UDP service name with the `service` parameter to display information about a specific service.
- Enter a UDP service port number with the `port` parameter to display information about a specific user-defined or well-known port.

### Examples

```
-> show ip udp relay
<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port</th>
<th>IP Address</th>
<th>Vlans</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS port</td>
<td>53</td>
<td>40.2.2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP port 54</td>
<td>54</td>
<td>20.2.2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UDP port 56</td>
<td>56</td>
<td></td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>TFTP port</td>
<td>69</td>
<td>200</td>
<td></td>
<td>20</td>
</tr>
</tbody>
</table>
```

```
-> show ip udp relay port 54
<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port</th>
<th>IP Address</th>
<th>Vlans</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
UDP port 54      54      20.2.2.1

-> show ip udp relay service tftp
      Service Name         Port   IP Address       Vlans   Services
      ---------------------+------+----------------+---------+---------------------
      TFTP port            69                      200           20

**Output Definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>The active UDP service name.</td>
</tr>
<tr>
<td>Port</td>
<td>The UDP service port number.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The destination IP address assigned to the UDP service port. Configured through the <code>ip udp relay address</code> command.</td>
</tr>
<tr>
<td>Vlans</td>
<td>The destination VLANs assigned to the UDP service port. Configured through the <code>ip udp relay vlan</code> command.</td>
</tr>
<tr>
<td>Services</td>
<td>The destination Shortest Path Bridging (SPB) service assigned to the UDP service port. Configured through the <code>ip udp relay svc</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 8.5R4; IP Address and Services field added.

**Related Commands**

`show ip udp relay statistics` Displays the current statistics for each UDP port relay service.

**MIB Objects**

N/A
show ip udp relay statistics

Displays the current statistics for each UDP port relay service. These statistics include the name of the service, the forwarding VLANs, Shortest Path Bridging (SPB) services, or an IP address configured for that service, and the number of packets the service has sent and received.

```
show ip udp relay statistics [service {tftp | tacacs | ntp | nbns | nbdd | dns}] [port [port_num]]
```

### Syntax Definitions

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **nbns**: NBNS well-known ports 137.
- **nbdd**: NBDD well-known port 138.
- **dns**: DNS well-known port 53.
- **port_num**: A user-defined or well-known UDP service port number.

### Defaults

By default, the statistics for all UDP services is shown.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

|-------|------|------|------|-------|------|-------|------|------|----------------+-----------------------------------------------|------|
|       | Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes            | Yes                                          | Yes  |

### Usage Guidelines

- Enter a UDP service name with the **service** parameter to display information about a specific service.
- Enter a UDP service port number with the **port** parameter to display information about a specific user-defined or well-known port.
- Use the **ip udp relay no statistics** command to reset statistics counters.

### Examples

```
-> show ip udp relay statistics
Port   Service        Pkts Recvd      Pkts Sent   Dst Vlan/IP Address    Svc
------+--------------+---------------+-----------+----------------------+-----------
9900  6900        10.1.1.2
53 DNS port    0          0             10.1.1.2
54 UDP port 54  0          0             10.1.1.2
55 UDP port 55  0          0             200
56 UDP port 56  0          0             200
```
DHCP Relay Commands

56 UDP port 56 0 0 20
69 TFTP port 0 0 1
0 0 300
0 0 200
69 TFTP port 0 0 20
123 NTP port 0 0 20.1.1.2

-> show ip udp relay statistics service tftp
Port Service Pkts Recvd Pkts Sent Dst Vlan/IP Address Svc
-----+--------------+---------------+-----------+----------------------+-----------
69 TFTP port 0 0 1
0 0 300
0 0 200
69 TFTP port 0 0 20

-> show ip udp relay statistics port 53
Port Service Pkts Recvd Pkts Sent Dst Vlan/IP Address Svc
-----+--------------+---------------+-----------+----------------------+-----------
53 DNS port 0 0 10.1.1.2

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The active UDP port number.</td>
</tr>
<tr>
<td>Service</td>
<td>The active UDP service name.</td>
</tr>
<tr>
<td>Pkts Recvd</td>
<td>The number of packets received by this service port from a client.</td>
</tr>
<tr>
<td>Pkts Sent</td>
<td>The number of packets sent from this service port to the server.</td>
</tr>
<tr>
<td>Dst Vlan/IP Address</td>
<td>The VLAN or IP address assigned to the UDP service port that forwards traffic destined for the port. Configured through the ip udp relay vlan or ip udp relay address command.</td>
</tr>
<tr>
<td>Svc</td>
<td>The SPB service assigned to the UDP service port that forwards traffic destined for the port. Configured through the ip udp relay svc command.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Release 8.5R4; Dst Vlan/IP Address and Svc fields added.

Related Commands

- **show ip udp relay** Displays current configuration for UDP services by service name or by service port number.
- **ipv6 udp relay clear statistics** Resets all the generic UDP Relay service statistics.

MIB Objects

N/A
ip udp relay no statistics

Resets all the generic UDP Relay service statistics.

Syntax Definitions

N/A

Defaults

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

When this command is applied, the UDP relay statistics are cleared and the show ip udp relay statistics command displays no information.

Examples

-> ip udp relay no statistics

Release History

Release 7.1.1; command introduced.

Related Commands

show ip udp relay statistics Displays the current statistics for each UDP port relay service.

MIB Objects

genericUdpServiceTable
genericUdpServiceStatReset
**ipv6 udp relay port**

Enables or disables generic IPv6 UDP relay for the specified UDP service port. A user-defined or well-known UDP port number is specified with this command.

```
ipv6 udp relay port port_num [description description]
ipv6 udp relay no port port_num
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port_num</td>
<td>A UDP service port number (for example, 53, 69, 301).</td>
</tr>
<tr>
<td>description</td>
<td>An optional description for the specified UDP service port.</td>
</tr>
</tbody>
</table>

### Defaults

By default, relay is enabled on the BOOTP/DHCP well-known ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to disable generic UDP relay for the specified port.
- Use the `ipv6 dhcp relay` commands to configure functionality for BOOTP/DHCP well-known ports (67/68).

### Examples

- `ipv6 udp relay port 54`
- `ipv6 udp relay port 54 description “Generic UDP Service”`
- `ipv6 udp relay no port 54`
- `ipv6 udp relay port 69 description “TFTP relay”`
- `ipv6 udp relay no port 69`

### Release History

Release 8.6R1; command introduced.
**Related Commands**

- **ipv6 udp relay vlan** Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.
- **ipv6 udp relay svc** Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded.
- **ipv6 udp relay address** Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.
- **show ipv6 udp relay** Displays the current configuration for UDP services by service name or by service port number.

**MIB Objects**

alaGenericUdpv6ServiceTable
  alaGenericUdpv6ServiceUdpPort
  alaGenericUdpv6ServiceDescription
  alaGenericUdpv6ServiceRowStatus
**ipv6 udp relay service**

Enables or disables generic IPv6 UDP relay for the specified UDP service name (DNS, NTP, or other well-known UDP ports).

```
ipv6 udp relay service {tftp | tacacs | ntp | dns} [description description]
ipv6 udp relay no service {tftp | tacacs | ntp | dns}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>tftp</td>
<td>TFTP well-known port 69.</td>
</tr>
<tr>
<td>tacacs</td>
<td>TACACS well-known port 65.</td>
</tr>
<tr>
<td>ntp</td>
<td>NTP well-known port 123.</td>
</tr>
<tr>
<td>dns</td>
<td>DNS well-known port 53.</td>
</tr>
<tr>
<td>description</td>
<td>An optional description for the specified UDP well-known service port.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to disable UDP Relay for the specified service port.
- The `description` parameter is used with any of the `service` keywords and provides a user-defined description to identify the port service.
- Note that when UDP port relay is enabled for NTP, relay cannot forward NTP packets that contain a destination IP address that matches a VLAN router IP address on the switch.

### Examples

- `-> ipv6 udp relay service dns`
- `-> ipv6 udp relay service dns description dns_1`
- `-> ipv6 udp relay no service dns`
Release History
Release 8.6R1; command introduced.

Related Commands

ipv6 udp relay vlan  Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.
ipv6 udp relay svc  Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP service port is forwarded.
ipv6 udp relay address  Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.
show ipv6 udp relay  Displays the current configuration for UDP services by service name or by service port number.

MIB Objects
alaGenericUdpv6ServiceTable
  alaGenericUdpv6ServiceUdpPort
  alaGenericUdpv6ServiceDescription
  alaGenericUdpv6ServiceRowStatus
**ipv6 udp relay vlan**

Specifies a VLAN on which traffic destined for the specified UDP service port is forwarded.

```
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port port_num [description description]} vlan vlan_id[-vlan_id2]
```

```
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port port_num} no vlan vlan_id[-vlan_id2]
```

### Syntax Definitions

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **dns**: DNS well-known port 53.
- **port_num**: A user-defined port number.
- **description**: A description of the UDP service.
- **vlan_id[-vlan_id2]**: VLAN ID number. Use a hyphen to specify a range of VLAN IDs (for example, 3-5).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the VLAN association with the UDP service port.
- The UDP port must be created before using this command.
- Use the **service** keyword to specify a well-known UDP service name. Use the **port** keyword to specify a user-defined or well-known UDP service port number.

### Examples

- `-> ipv6 udp relay service dns vlan 10`
- `-> ipv6 udp relay service dns vlan 500-550`
- `-> ipv6 udp relay service dns no vlan 10`
- `-> ipv6 udp relay port 3047 vlan 20`
- `-> ipv6 udp relay port 3047 no vlan 20`
**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- **ipv6 udp relay port**
  Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.

- **ipv6 udp relay service**
  Enables or disables generic UDP relay for well-known UDP service names.

- **ipv6 udp relay svc**
  Specifies a Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded.

- **ipv6 udp relay address**
  Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.

- **show ipv6 udp relay**
  Displays the current configuration for UDP services by service name or by service port number.

**MIB Objects**

- `alaGenericUdpv6ServiceDstTable`
  - `alaGenericUdpv6ServiceDstType`
  - `alaGenericUdpv6ServiceDstPort`
  - `alaGenericUdpv6ServiceDstId`
  - `alaGenericUdpv6ServiceDstDescription`
  - `alaGenericUdpv6ServiceDstRowStatus`
**ipv6 udp relay svc**

Specifies a Shortest Path Bridging (SPB) service on which traffic destined for a UDP port is forwarded.

```plaintext
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port port_num [description description]} svc service_id[-service_id2]
```

```plaintext
ipv6 udp relay service {tftp | tacacs | ntp | dns} | port port_num no svc service_id[-service_id2]
```

### Syntax Definitions

- **tftp**
  - TFTP well-known port 69.
- **tacacs**
  - TACACS well-known port 65.
- **ntp**
  - NTP well-known port 123.
- **dns**
  - DNS well-known port 53.
- **port_num**
  - A user-defined port number.
- **description**
  - A description of the UDP service.
- **service_id[-service_id2]**
  - SPB service ID number. Use a hyphen to specify a range of service IDs (3-5).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the SPB service association with the UDP service port.
- The UDP port must be created before using this command.
- Use the `service` keyword to specify a well-known UDP service name. Use the `port` keyword to specify a user-defined or well-known UDP service port number.

### Examples

- `ipv6 udp relay service dns svc 10`
- `ipv6 udp relay service dns svc 50-55`
- `ipv6 udp relay service dns no svc 10`
- `ipv6 udp relay port 3047 svc 20`
- `ipv6 udp relay port 3047 no svc 20`
**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- `ipv6 udp relay port` Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
- `ipv6 udp relay service` Enables or disables generic UDP relay for well-known UDP service names.
- `ipv6 udp relay vlan` Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.
- `ipv6 udp relay address` Specifies the UDP server IPv6 address to which traffic destined for the specified UDP port is forwarded as unicast packets.
- `show ipv6 udp relay` Displays the current configuration for UDP services by service name or by service port number.

**MIB Objects**

- `alaGenericUdpv6ServiceDstTable`
  - `alaGenericUdpv6ServiceDstType`
  - `alaGenericUdpv6ServiceDstPort`
  - `alaGenericUdpv6ServiceDstId`
  - `alaGenericUdpv6ServiceDstDescription`
  - `alaGenericUdpv6ServiceDstRowStatus`
**ipv6 udp relay address**

Specifies the UDP server IPv6 address to which traffic destined for a UDP port is forwarded as unicast packets.

```plaintext
ipv6 udp relay {service {tftp | tacacs | ntp | dns} | port port_num [description description]} address ipv6_address
```

```plaintext
ipv6 udp relay service {tftp | tacacs | ntp | dns} | port port_num no address ip6_address
```

### Syntax Definitions

- **tftp**: TFTP well-known port 69.
- **tacacs**: TACACS well-known port 65.
- **ntp**: NTP well-known port 123.
- **dns**: DNS well-known port 53.
- **port_num**: A user-defined port number.
- **description**: A description of the UDP service.
- **ipv6_address**: The IPv6 address of a UDP server.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the IPv6 address association with the UDP service port.
- The UDP port must be created before using this command.
- Only one IPv6 address can be configured for a UDP port (multiple IPv6 addresses for the same UDP port is not supported).
- Use the `service` keyword to specify a well-known UDP service name. Use the `port` keyword to specify a user-defined or well-known UDP service port number.
- When the specified UDP port is associated with an IPv6 address, the relay is operating at the Layer 3 level; any attempt to then assign a VLAN or SPB service to that UDP port is blocked. UDP ports associated with a VLAN or SPB service are operating at the Layer 2 level.
**Examples**

-> ipv6 udp relay service dns address 2001:DB8:3001::3
-> ipv6 udp relay service tftp address 2001:DB8:3001::3
-> ipv6 udp relay service dns no address 2001:DB8:3001::3
-> ipv6 udp relay port 3047 address 2001:DB8:3001::3
-> ipv6 udp relay port 3047 no address 2001:DB8:3001::3

-> ipv6 udp relay port 54 address 30.2.2.1
-> ipv6 udp relay port 54 vlan 200
ERROR: UDP port configured in L3 mode

-> ipv6 udp relay port 64 vlan 200
-> ipv6 udp relay port 64 address 40.2.2.1
ERROR: UDP port configured in L2 mode

**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- **ipv6 udp relay port** Enables or disables generic UDP relay for user-defined or well-known UDP service port numbers.
- **ipv6 udp relay service** Enables or disables generic UDP relay for well-known UDP service names.
- **ipv6 udp relay vlan** Specifies the VLAN on which traffic destined for the specified UDP port is forwarded.
- **ipv6 udp relay svc** Specifies the Shortest Path Bridging (SPB) service on which traffic destined for the specified UDP port is forwarded.
- **show ipv6 udp relay** Displays the current configuration for UDP services by service name or by service port number.

**MIB Objects**

alaGenericUdpv6ServiceDstIpTable
- alaGenericUdpv6ServiceDstUdpPort
- alaGenericUdpv6ServiceDstIpType
- alaGenericUdpv6ServiceDstIpAddress
- alaGenericUdpv6ServiceDstIpRowStatus
show ipv6 udp relay

Displays the generic UDP relay service configuration.

show ipv6 udp relay [service {tftp | tacacs | ntp | dns} | port port_num]

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tftp</td>
<td>TFTP well-known port 69.</td>
</tr>
<tr>
<td>tacacs</td>
<td>TACACS well-known port 65.</td>
</tr>
<tr>
<td>ntp</td>
<td>NTP well-known port 123.</td>
</tr>
<tr>
<td>dns</td>
<td>DNS well-known port 53.</td>
</tr>
<tr>
<td>port_num</td>
<td>A user-defined or well-known port number.</td>
</tr>
</tbody>
</table>

Defaults

By default, the configuration for all UDP services is shown.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Enter a UDP service name with the service parameter to display information about a specific service.
- Enter a UDP service port number with the port parameter to display information about a specific user-defined or well-known port.

Examples

- show ipv6 udp relay
  Service Name     Port  IPv6 Address    Vlans/Services
  ----------------+-------+------------------+---------------
  DNS port        53     3001::3          
  UDP port 137    137    123             200

- show ipv6 udp relay port 69
  Service Name     Port  IPv6 Address    Vlans/Services
  ----------------+-------+------------------+---------------
  TFTP port       69     110             
  TFTP port       69     120             
  TFTP port       69     200             
  TFTP port       69     200             
-> show ipv6 udp relay service dns

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port</th>
<th>IPv6 Address</th>
<th>Vlans/Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS port</td>
<td>53</td>
<td>3001::3</td>
<td></td>
</tr>
</tbody>
</table>

**Release History**
Release 8.6R1; command introduced.

**Related Commands**
- **show ipv6 udp relay statistics** Displays the current statistics for each UDP port relay service.

**MIB Objects**
- **N/A**
**show ipv6 udp relay statistics**

Displays the current statistics for each UDP port relay service. These statistics include the name of the service, the forwarding VLANs, Shortest Path Bridging (SPB) services, or an IPv6 address configured for that service, and the number of packets the service has sent and received.

```
show ipv6 udp relay statistics [service {tftp | tacacs | ntp | dns}] [port [port_num]]
```

### Syntax Definitions

- **tftp**  
  TFTP well-known port 69.
- **tacacs**  
  TACACS well-known port 65.
- **ntp**  
  NTP well-known port 123.
- **dns**  
  DNS well-known port 53.
- **port_num**  
  A user-defined or well-known UDP service port number.

### Defaults

By default, the statistics for all UDP services is shown.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a UDP service name with the `service` parameter to display information about a specific service.
- Enter a UDP service port number with the `port` parameter to display information about a specific user-defined or well-known port.
- Use the `ipv6 udp relay clear statistics` command to reset statistics counters.

### Examples

```
-> show ipv6 udp relay statistics
Port Service    Pkts Recvd Pkts Sent  Dst Vlan/Svc/IPv6 Address
---------------------------------------------
53 DNS port     0    0 3001::2
54 UDP port 54   0    0 10
55 UDP port 55   0    0 200
56 UDP port 56   0    0 200
69 TFTP port     0    0 1
                 0    0 3000
                 0    0 200
```
show ipv6 udp relay statistics

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Pkts Recvd</th>
<th>Pkts Sent</th>
<th>Dst Vlan/Svc/IPv6 Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>69 TFTP port</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2001::2</td>
</tr>
<tr>
<td>123 NTP port</td>
<td>0</td>
<td>0</td>
<td>300</td>
<td>2001::2</td>
</tr>
<tr>
<td>69 TFTP port</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>2001::2</td>
</tr>
</tbody>
</table>

show ipv6 udp relay statistics service tftp

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Pkts Recvd</th>
<th>Pkts Sent</th>
<th>Dst Vlan/Svc/IPv6 Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>53 DNS port</td>
<td>0</td>
<td>0</td>
<td>300</td>
<td>3001::2</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The active UDP port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>The active UDP service name.</td>
</tr>
<tr>
<td>Pkts Recvd</td>
<td>The number of packets received by this service port from a client.</td>
</tr>
<tr>
<td>Pkts Sent</td>
<td>The number of packets sent from this service port to the server.</td>
</tr>
<tr>
<td>Dst Vlan/Ip Address</td>
<td>The VLAN or IPv6 address assigned to the UDP service port that forwards traffic destined for the port. Configured through the <code>ipv6 udp relay vlan</code> or <code>ipv6 udp relay address</code> command.</td>
</tr>
<tr>
<td>Svc</td>
<td>The SPB service assigned to the UDP service port that forwards traffic destined for the port. Configured through the <code>ipv6 udp relay svc</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R1; command introduced.

Related Commands

show ipv6 udp relay
Displays current configuration for UDP services by service name or by service port number.

ipv6 udp relay clear statistics
Resets all the generic UDP Relay service statistics.

MIB Objects

N/A
**ipv6 udp relay clear statistics**

Resets all the generic UDP Relay service statistics.

### Syntax Definitions

N/A

### Defaults

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900V72/C32</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When this command is applied, all UDP relay statistics are reset to zero.
- Use the `show ipv6 udp relay statistics` command to display UDP relay statistics.

### Examples

```
-> ipv6 udp relay clear statistics
```

### Release History

Release 8.6R1; command introduced.

### Related Commands

- `show ipv6 udp relay statistics` Displays the current statistics for each UDP port relay service.

### MIB Objects

- `alaGenericUdpv6ServiceGlobal`
- `alaGenericUdpv6ServiceStatReset`
ipv6 dhcp relay admin-state

Enables or disables the DHCPv6 Relay feature on a per-VRF basis.

ipv6 dhcp relay admin-state {enable | disable}

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the DHCPv6 Relay feature.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the DHCPv6 Relay feature.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

DHCPv6 Relay must be explicitly enabled on the interfaces from which received DHCP client messages are to be relayed.

**Examples**

- `-> ipv6 dhcp relay admin-state enable`
- `-> ipv6 dhcp relay admin-state disable`

**Release History**

Release 7.3.4; command introduced.
**Related Commands**

- `ipv6 dhcp relay interface admin-state`
  Enables or disables the relay of DHCPv6 client messages received on an interface.

- `show ipv6 dhcp relay`
  Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

**MIB Objects**

- `alaDHCPv6Config`
  - `alaDHCPv6RelayAdminStatus`
ipv6 dhcp relay interface admin-state

Enables or disables the relay of DHCPv6 client messages received on an interface.

`ipv6 dhcp relay if_name admin-state {enable | disable}

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_name</td>
<td>IPv6 interface name.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables the relay of DHCPv6 client messages on an interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the relay of DHCPv6 client messages on an interface.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

At least one relay destination must be configured before enabling the DHCPv6 relay on an interface.

### Examples

`-> ipv6 dhcp relay int1 admin-state enable`

`-> ipv6 dhcp relay int1 admin-state disable`

### Release History

Release 7.3.4; command introduced.
**Related Commands**

- **ipv6 dhcp relay destination**  
  Configures the DHCPv6 relay destination.

- **show ipv6 dhcp relay**  
  Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

**MIB Objects**

- alaDHCPv6RelayInterfaceTable
- alaDHCPv6RelayInterfaceAdminStatus
**ipv6 dhcp relay destination**

Configures the DHCPv6 Relay destination.

```
ipv6 dhcp relay if_name destination ip6_address scope_if_name
no ipv6 dhcp relay if_name destination ip6_address scope_if_name
```

### Syntax Definitions

- **if_name**: IPv6 interface name.
- **ip6_address**: The IPv6 address of the relay destination.
- **scope_if_name**: Name of the interface for the local-link. This must be specified if the relay destination is a link-local. Not required if the destination address is not a link-local address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Maximum of five relay destinations can be configured for an interface.
- If the relay destination is a link-local address, the name of the interface used to reach the destination must be specified.
- Use the `no` form of the command to remove the configured DHCPv6 Relay destination for an interface.
- The IPv6 interface must be defined for a VLAN or a Shortest Path Bridging (SPB) service before using this command. Packets destined for the specified IPv6 address are relayed over the VLAN or SPB service domain.
- Configuring a DHCPv6 Relay agent for an IPv6 interface that is bound to an SPB service (a service-based IPv6 interface) is supported only on the OmniSwitch 9900.

### Examples

```
-> ipv6 dhcp relay int1 destination 2001:DB8:3001::3
-> ipv6 dhcp relay int1 destination fe80::64 int1
-> no ipv6 dhcp relay int1 destination 2001:DB8:3001::3
```
**Release History**

Release 7.3.4; command introduced.

**Related Commands**

`show ipv6 dhcp relay`  Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

**MIB Objects**

`alaDHCPv6RelayDestinationTable`  
`alaDHCPv6RelayDestinationAddressType`  
`alaDHCPv6RelayDestinationAddress`  
`alaDHCPv6RelayDestinationRowStatus`
**ipv6 dhcp relay maximum-hops**

Sets the maximum number of hops value for the DHCPv6 Relay configuration. This value specifies the maximum number of relays a DHCPv6 packet is allowed to traverse until it reaches its server destination. Limiting the number of hops that can forward a packet prevents packets from looping through the network.

`ipv6 dhcp relay maximum-hops hops`

**Syntax Definitions**

`hops` The maximum number of relays. The valid range is 1–32.

**Defaults**

By default, the maximum hops value is set to 32 hops.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a packet contains a hop count equal to or greater than the `hops` value, DHCPv6 Relay discards the packet.
- The maximum hops value only applies to DHCPv6 Relay and is ignored by other services.

**Examples**

`-> ipv6 dhcp relay maximum-hops 1`

`-> ipv6 dhcp relay maximum-hops 10`

**Release History**

Release 8.6R1; command introduced.
Related Commands

- `ipv6 dhcp relay admin-state`  Enables or disables the DHCP Relay feature for the switch.
- `show ipv6 dhcp relay`  Displays all the interface on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

MIB Objects

- `alaDHCPv6RelayConfig`
- `alaDHCPv6RelayMaximumHops`
**show ipv6 dhcp relay**

Displays all the interfaces on which the DHCPv6 relay is configured, the relay destinations, and the status of the DHCPv6 relay.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Interfaces on which DHCPv6 relay is disabled and which have no relay destinations configured will not be shown in the output.

**Examples**

```
-> show ipv6 dhcp relay
DHCPv6 Relay: Enabled
Maximum Hops: 32

Interface                   Relay Destination(s)                      Status
---------------------------+-----------------------------------------+--------
vlan-41                     ff02::1:2                                 Enabled
vlan-103                    2001:dbc8:8003::17                        Disabled
                              2001:dbc8:8004::99
vlan-200                    fe80::cd0:deff:fe28:1ca5 vlan-201         Enabled
                              tunnel-2 2001:dbc8:a23::ea77
```

**output definitions**

- **DHCPv6 Relay**: Specifies if the DHCPv6 Relay feature is enabled in the current VRF.
- **Maximum Hops**: The maximum number of relays the BOOTP/DHCP packet can go through until it reaches its server destination.
- **Interface**: Displays the interface on which DHCPv6 Relay is enabled.
output definitions

<table>
<thead>
<tr>
<th>Relay Destination(s)</th>
<th>Displays the configured DHCPv6 Relay destination(s) for the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays the status of DHCPv6 Relay on the interface.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command introduced.
Release 8.6R1; “Maximum Hops” field added.

Related Commands

ipv6 dhcp relay admin-state
ipv6 dhcp relay interface admin-state
ipv6 dhcp relay destination
ipv6 dhcp relay maximum-hops

Enables or disables the DHCPv6 Relay feature on a per-VRF basis.
Enables or disables the relay of DHCPv6 client messages received on an interface.
Configures the DHCPv6 relay destination address.
Configures the maximum number of hops value.

MIB Objects

alaDHCPv6RelayConfig
alaDHCPv6RelayMaximumHops
alaDHCPv6RelayAdminStatus
alaDHCPv6RelayInterfaceTable
alaDHCPv6RelayInterfaceEntry
alaDHCPv6RelayInterfaceAdminStatus
alaDHCPv6RelayDestinationTable
alaDHCPv6RelayDestinationAddress
**dhcp-server**

Enables or disables the DHCP server operation.

`dhcp-server {enable | disable}`

---

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the DHCP server.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the DHCP server.</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When DHCP server is enabled on the switch, DHCP relay and DHCP snooping will not be supported on the default VRF of the switch.

- DHCP server must be restarted when changes are made to the dhcpd.conf or dhcpd.pcy file. Use the `dhcp-server restart` command to restart the DHCP server.

### Examples

```
-> dhcp-server enable
-> dhcp-server disable
```

### Release History

Release 7.3.4; command was introduced.
Related Commands

- **show dhcp-server leases** Displays the leases offered by the DHCP server.
- **dhcpp-server restart** Allows to restart the DHCP server when the `dhcpp.conf` or `dhcpp.pcy` file is modified.
- **clear dhcp-server statistics** Clears the statistics of the DHCP server.

MIB Objects

- `alaDhcpSrvGlobalConfigStatus`
**dhcp-server restart**

Allows to restart the DHCP server when the dhcpd.conf or dhcpd.pcy file is modified.

```
dhcp-server restart
```

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>restart</th>
<th>Reverts the DHCP server.</th>
</tr>
</thead>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The command can be used to restart the DHCP server when the dhcpd.conf or dhcpd.pcy file is modified.

**Examples**

```
-> dhcp-server restart
```

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- **dhcp-server**  
  Enables or disables the DHCP server operation

**MIB Objects**

alaDhcpSrvGlobalRestart
show dhcp-server leases

Displays the leases offered by the DHCP server.

```
show dhcp-server leases [ip- address ip_address | mac-address mac_address] [type {static | dynamic}] [count]
```

### Syntax Definitions

- **ip_address**: Specifies IP address of the interface configured with DHCP server.
- **mac_address**: Specifies MAC address of the interface configured with DHCP server.
- **static**: Displays only static leases.
- **dynamic**: Displays only dynamic leases.
- **count**: Count of DHCP messages recorded.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

DHCP server should be enabled before using this command.

### Examples

```
-> show dhcp-server leases

Total leases: 8

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC address</th>
<th>Lease Granted</th>
<th>Lease Expiry</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.0.1.1</td>
<td>00:00:01:b8:91:3f</td>
<td>DEC 15 14:10:59 2009</td>
<td>DEC 19 01:30:59 2009</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>200.0.1.2</td>
<td>00:00:01:b8:91:37</td>
<td>DEC 15 14:11:05 2009</td>
<td>DEC 19 01:31:05 2009</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>200.0.1.3</td>
<td>00:00:01:b8:91:3b</td>
<td>DEC 15 14:11:48 2009</td>
<td>DEC 19 01:31:48 2009</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>200.0.1.4</td>
<td>00:00:01:b8:91:3d</td>
<td>DEC 15 14:11:53 2009</td>
<td>DEC 19 01:31:53 2009</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>220.0.0.2</td>
<td>00:00:01:1d:4f:7e</td>
<td>DEC 15 14:11:45 2009</td>
<td>DEC 15 22:31:45 2009</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>220.0.0.3</td>
<td>00:00:01:5a:0b:76</td>
<td>DEC 15 14:12:00 2009</td>
<td>DEC 15 22:32:00 2009</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>220.0.0.4</td>
<td>00:00:01:1d:4f:7d</td>
<td>DEC 15 14:11:53 2009</td>
<td>DEC 15 22:31:53 2009</td>
<td>DYNAMIC</td>
</tr>
<tr>
<td>120.0.0.4</td>
<td>00:00:02:12:4f:8c</td>
<td>DEC 15 14:11:53 2009</td>
<td>DEC 15 23:31:53 2009</td>
<td>STATIC</td>
</tr>
</tbody>
</table>
-> show dhcp-server leases ip-address 200.0.1.2

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC address</th>
<th>Lease Granted</th>
<th>Lease Expiry</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.0.1.2</td>
<td>00:00:01:b8:91:37</td>
<td>DEC 15 14:11:05 2009</td>
<td>DEC 19 01:31:05 2009</td>
<td>DYNAMIC</td>
</tr>
</tbody>
</table>

> show dhcp-server leases mac-address 00:00:01:1d:4f:7d

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC address</th>
<th>Lease Granted</th>
<th>Lease Expiry</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>220.0.0.4</td>
<td>00:00:01:1d:4f:7d</td>
<td>DEC 15 14:11:53 2009</td>
<td>DEC 15 22:31:53 2009</td>
<td>DYNAMIC</td>
</tr>
</tbody>
</table>

> show dhcp-server leases type static

Total leases: 1

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC address</th>
<th>Lease Granted</th>
<th>Lease Expiry</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>120.0.0.4</td>
<td>00:00:02:12:4f:8c</td>
<td>DEC 15 14:11:53 2009</td>
<td>DEC 15 23:31:53 2009</td>
<td>STATIC</td>
</tr>
</tbody>
</table>

**output definitions**

- **IP address**: The IP address allocated to the client.
- **MAC address**: The MAC address of the client for which the lease is allocated.
- **Lease Granted**: The date and time at which lease is granted.
- **Lease Expiry**: The date and time at which lease expires.
- **Type**: The type of lease offered.

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- **clear dhcp-server statistics**: Clears the DHCP server lease statistics.

**MIB Objects**

- alaDhcpSrvLeaseTable
  - alaDhcpSrvLeaseMACAddress
  - alaDhcpSrvLeaseIpAddress
  - alaDhcpSrvLeaseLeaseGrant
  - alaDhcpSrvLeaseLeaseExpiry
  - alaDhcpSrvLeaseType
show dhcp-server statistics

Displays the statistics of the DHCP server.

show dhcp-server statistics [packets | hosts | subnets | all]

Syntax Definitions

packets Displays general statistical information along with specific information about data packets received, dropped, and transmitted.

hosts Displays general statistical information along with specific information about leases related to the DHCP server.

subnets Displays general statistical information along with specific information about all the subnets.

all Displays all statistical information related to the DHCP server.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

DHCP server should be enabled before using this command.

Examples

-> show dhcp-server statistics
General:
DHCP Server Name: mample.vitalqip.com,
DHCP Server Status : Enabled,
Total Subnets Managed : 7,
Total Subnets Used : 2,
Total Subnets Unused : 5,
Total Subnets Full : 0,
DHCP Server System Up Time : TUE DEC 15 14:10:27.9956
Lease DB Sync time (in sec) : 60,
   Last sync time : TUE DEC 15 14:21:34 2009,
   Next sync time : TUE DEC 15 14:22:34 2009

-> show dhcp-server statistics packets
Packets:
Total DHCP Discovers : 12,
Total DHCP Offers : 12,
Total DHCP Requests : 16,
Total DHCP Request Grants : 10,
Total DHCP Request Renews : 6,
Total DHCP Declines : 0,
Total DHCP Acks : 16,
Total DHCP Nacks : 0,
Total DHCP Releases : 0,
Total DHCP Informs : 0,
Total Bootp requests : 0,
Total Bootp response : 0,
Total Unknown packets : 0

-> show dhcp-server statistics hosts
Leases:
  Total:
    Leases Managed: 1365,
    Leases used : 7,
    Leases unused : 1358,
    Leases Pending : 0,
    Leases unavailable : 0
Static DHCP:
  Leases Managed : 0,
  Leases used : 0,
  Leases unused : 0,
  Leases Pending : 0,
  Leases unavailable : 0
Dynamic DHCP:
  Leases Managed : 1365,
  Leases used : 7,
  Leases unused : 1358,
  Leases Pending : 0,
  Leases unavailable : 0
Automatic DHCP:
  Leases Managed : 0,
  Leases used : 0,
  Leases unused : 0,
  Leases Pending : 0,
  Leases unavailable : 0
Static Bootp:
  Leases Managed : 0,
  Leases used : 0,
  Leases unused : 0,
  Leases Pending : 0,
  Leases unavailable : 0
Automatic Bootp :
  Leases Managed : 0,
  Leases used : 0,
  Leases unused : 0,
  Leases Pending : 0,
  Leases unavailable : 0

-> show dhcp-server statistics subnets
Subnets:
  Subnet1:
    Subnet: 200.0.0.0,
    Total : 1022,
    Static DHCP : 0,
DHCP Relay Commands

show dhcp-server statistics

Dynamic DHCP : 1022,
Automatic DHCP : 0,
Static Bootp : 0,
Automatic Bootp : 0
Ranges:
   Start : 200.0.1.1,
   End   : 200.0.2.255,
   Mask  : 255.255.253.0,
   Type  : 5,
   Used  : 4,
   Unused : 507,
   Pending : 0,
  Unavailable : 0

Subnet2:
Subnet : 220.0.0.0,
Total : 508,
Static DHCP : 0,
Dynamic DHCP : 508,
Automatic DHCP : 0,
Static Bootp : 0,
Automatic Bootp : 0
Ranges:
   Start : 220.0.0.2,
   End   : 220.0.0.255,
   Mask  : 255.255.255.0,
   Type  : 5,
   Unused : 251,
   Used   : 3,
   Pending : 0,
   Unavailable : 0

Subnet3:
Subnet : 150.0.0.0,
Total : 400,
Static DHCP : 0,
Dynamic DHCP : 400,
Automatic DHCP : 0,
Static Bootp : 0,
Automatic Bootp : 0
Ranges:
   Range1:
      Start : 150.0.1.1,
      End   : 150.0.1.100,
      Mask  : 255.255.255.0,
      Type  : 5,
      Used  : 0,
      Unused : 100,
      Pending : 0,
      Unavailable : 0
   Range2:
      Start : 150.0.2.1,
      End   : 150.0.2.100,
      Mask  : 255.255.255.0,
      Type  : 5,
      Unused : 100,
      Used   : 0,
      Pending : 0,
      Unavailable : 0

Subnet4:
Subnet : 50.0.0.0,
DHCP Relay Commands

- show dhcp-server statistics

Total : 200,
Static DHCP : 0,
Dynamic DHCP : 200,
Automatic DHCP : 0,
Static Bootp : 0,
Automatic Bootp : 0

Ranges:
Start : 50.0.1.1,
End : 50.0.1.100,
Mask : 255.255.255.0,
Type : 5,
Unused : 100,
Used : 0,
Pending : 0,
Unavailable : 0

-> show dhcp-server statistics all

General:
DHCP Server Name: mample.vitalqip.com,
DHCP Server Status : Enabled,
Total Subnets Managed : 7,
Total Subnets Used : 2,
Total Subnets Unused : 5,
Total Subnets Full : 0,
DHCP Server System Up Time : TUE DEC 15 14:10:27.9956

Lease DB Sync:
  DB Sync time (in sec) : 60,
  Last sync time : TUE DEC 15 14:21:34 2009,
  Next sync time : TUE DEC 15 14:22:34 2009

Packets:
Total DHCP Discovers: 12,
Total DHCP Offers : 12,
Total DHCP Requests : 16,
Total DHCP Request Grants : 10,
Total DHCP Request Renew : 6,
Total DHCP Declines : 0,
Total DHCP Acks : 16,
Total DHCP Nacks : 0,
Total DHCP Releases : 0,
Total DHCP Informs : 0,
Total Bootp requests : 0,
Total Bootp response : 0,
Total Unknown packets : 0

Leases:
Total:
  Leases Managed: 1365,
  Leases used : 7,
  Leases unused : 1358,
  Leases Pending : 0,
  Leases unavailable : 0

Static DHCP:
  Leases Managed : 0,
  Leases used : 0,
  Leases unused : 0,
  Leases Pending : 0,
  Leases unavailable : 0

Dynamic DHCP:
  Leases Managed : 1365,
  Leases used : 7,
### DHCP Relay Commands

Show DHCP Server Statistics

<table>
<thead>
<tr>
<th>Leases used</th>
<th>1358,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leases Pending</td>
<td>0,</td>
</tr>
<tr>
<td>Leases unavailable</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Automatic DHCP:

<table>
<thead>
<tr>
<th>Leases Managed</th>
<th>0,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leases used</td>
<td>0,</td>
</tr>
<tr>
<td>Leases unused</td>
<td>0,</td>
</tr>
<tr>
<td>Leases Pending</td>
<td>0,</td>
</tr>
<tr>
<td>Leases unavailable</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Static Bootp:

<table>
<thead>
<tr>
<th>Leases Managed</th>
<th>0,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leases used</td>
<td>0,</td>
</tr>
<tr>
<td>Leases unused</td>
<td>0,</td>
</tr>
<tr>
<td>Leases Pending</td>
<td>0,</td>
</tr>
<tr>
<td>Leases unavailable</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Static Bootp:

<table>
<thead>
<tr>
<th>Leases Managed</th>
<th>0,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leases used</td>
<td>0,</td>
</tr>
<tr>
<td>Leases unused</td>
<td>0,</td>
</tr>
<tr>
<td>Leases Pending</td>
<td>0,</td>
</tr>
<tr>
<td>Leases unavailable</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Subnets:

**Subnet1:**

<table>
<thead>
<tr>
<th>Subnet</th>
<th>200.0.0.0,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>1022,</td>
</tr>
<tr>
<td>Static DHCP</td>
<td>0,</td>
</tr>
<tr>
<td>Dynamic DHCP</td>
<td>1022,</td>
</tr>
<tr>
<td>Automatic DHCP</td>
<td>0,</td>
</tr>
<tr>
<td>Static Bootp</td>
<td>0,</td>
</tr>
<tr>
<td>Automatic Bootp</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Ranges:

<table>
<thead>
<tr>
<th>Start</th>
<th>200.0.0.1,</th>
</tr>
</thead>
<tbody>
<tr>
<td>End</td>
<td>200.0.0.2,55</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.253.0,</td>
</tr>
<tr>
<td>Type</td>
<td>5,</td>
</tr>
<tr>
<td>Unused</td>
<td>507,</td>
</tr>
<tr>
<td>Pending</td>
<td>0,</td>
</tr>
<tr>
<td>Unavailable</td>
<td>0,</td>
</tr>
</tbody>
</table>

**Subnet2:**

<table>
<thead>
<tr>
<th>Subnet</th>
<th>220.0.0.0,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>508,</td>
</tr>
<tr>
<td>Static DHCP</td>
<td>0,</td>
</tr>
<tr>
<td>Dynamic DHCP</td>
<td>508,</td>
</tr>
<tr>
<td>Automatic DHCP</td>
<td>0,</td>
</tr>
<tr>
<td>Static Bootp</td>
<td>0,</td>
</tr>
<tr>
<td>Automatic Bootp</td>
<td>0</td>
</tr>
</tbody>
</table>

#### Ranges:

<table>
<thead>
<tr>
<th>Start</th>
<th>220.0.0.2,</th>
</tr>
</thead>
<tbody>
<tr>
<td>End</td>
<td>220.0.0.2,55</td>
</tr>
<tr>
<td>Mask</td>
<td>255.255.255.0,</td>
</tr>
<tr>
<td>Type</td>
<td>5,</td>
</tr>
<tr>
<td>Unused</td>
<td>251,</td>
</tr>
<tr>
<td>Used</td>
<td>3,</td>
</tr>
<tr>
<td>Pending</td>
<td>0,</td>
</tr>
<tr>
<td>Unavailable</td>
<td>0,</td>
</tr>
</tbody>
</table>

**Subnet3:**

<table>
<thead>
<tr>
<th>Subnet</th>
<th>150.0.0.0,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>400,</td>
</tr>
</tbody>
</table>
DHCP Relay Commands

show dhcp-server statistics

Static DHCP : 0,
Dynamic DHCP : 400,
Automatic DHCP : 0,
Static Bootp : 0,
Automatic Bootp : 0

Ranges:
  Range1:
    Start : 150.0.1.1,
    End   : 150.0.1.100,
    Mask  : 255.255.255.0,
    Type  : 5,
    Used  : 0,
    Unused : 100,
    Pending : 0,
    Unavailable : 0
  Range2:
    Start : 150.0.2.1,
    End   : 150.0.2.100,
    Mask  : 255.255.255.0,
    Type  : 5,
    Unused : 100,
    Used   : 0,
    Pending : 0,
    Unavailable : 0

Subnet4:
  Subnet : 50.0.0.0,
  Total  : 200,
  Static DHCP : 0,
  Dynamic DHCP : 200,
  Automatic DHCP : 0,
  Static Bootp : 0,
  Automatic Bootp : 0

Ranges:
  Start : 50.0.1.1,
  End   : 50.0.1.100,
  Mask  : 255.255.255.0,
  Type  : 5,
  Unused : 100,
  Used   : 0,
  Pending : 0,
  Unavailable : 0

output definitions

General stats Denotes general DHCP Server statistics.
Name Specifies the name assigned to the DHCP server.
Status Specifies up or down status of the DHCP server.
Total subnets used Specifies the total number of subnets being used.
Total subnets managed Specifies the total number of subnets being managed by the DHCP server.
Total subnets unused Specifies the total number of subnets being unused.
Total subnets full Specifies the total number of subnets where all the IP addresses are used.
DHCP Server System Up Time Shows the DHCP Server System Up Time Performance Monitor counter.
### Output Definitions (Continued)

<table>
<thead>
<tr>
<th>Output Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sync time</td>
<td>Specifies the time for DHCP server to contact and synchronize with the designated time server.</td>
</tr>
<tr>
<td>Last sync time</td>
<td>Specifies the last time the synchronization occurred.</td>
</tr>
<tr>
<td>Next sync time</td>
<td>Specifies the next time the synchronization should be scheduled.</td>
</tr>
<tr>
<td>Packet stats</td>
<td>Denotes statistical information about the data packet transmission.</td>
</tr>
<tr>
<td>Total DHCP Discovers</td>
<td>Specifies the total number of DHCPDISCOVER packets sent by the clients to the DHCP server.</td>
</tr>
<tr>
<td>Total DHCP Offers</td>
<td>Specifies the total number of DHCPOFFER packets sent by the server to the clients.</td>
</tr>
<tr>
<td>Total DHCP Requests</td>
<td>Specifies the total number of DHC普REQUEST packets sent by the clients in response to the DHCPOFFER packets.</td>
</tr>
<tr>
<td>Total DHCP Request Grants</td>
<td>Specifies the total number of DHCP request grants provided by the server to the clients.</td>
</tr>
<tr>
<td>Total DHCP Request Renews</td>
<td>Specifies the total number of DHCP lease renew requests sent by the clients to the DHCP server.</td>
</tr>
<tr>
<td>Total DHCP Declines</td>
<td>Specifies the total number of DHCP requests declined by the DHCP server.</td>
</tr>
<tr>
<td>Total DHCP Acks</td>
<td>Specifies the total number of DHCPACK acknowledgement packets sent by the DHCP server to the clients.</td>
</tr>
<tr>
<td>Total DHCP Nacks</td>
<td>Specifies the total number of DHCP Negative acknowledgements sent from the DHCP server to the clients. The DHCPNACK message is sent when all the IP addresses available to the server are exhausted and the client sends a DHCPREQUEST.</td>
</tr>
<tr>
<td>Total DHCP Releases</td>
<td>Specifies the total number of DHCPRELEASE packets sent by the DHCP server to release IP addresses from its clients.</td>
</tr>
<tr>
<td>Total DHCP Informs</td>
<td>Specifies the total number of DHCPINFORM packets sent by the clients to obtain DHCP options from the DHCP server.</td>
</tr>
<tr>
<td>Total Bootp requests</td>
<td>Specifies the total number of BOOTP requests sent by the clients to the DHCP server.</td>
</tr>
<tr>
<td>Total Bootp response</td>
<td>Specifies the total number of BOOTP response packets sent by the DHCP server to the clients.</td>
</tr>
<tr>
<td>Total Unknown packets</td>
<td>Specifies the total number of unknown or badly formatted DHCP packets received by the DHCP server.</td>
</tr>
<tr>
<td>Leases stats</td>
<td>Denotes statistical information about leases provided by the DHCP server.</td>
</tr>
<tr>
<td>Hosts Managed</td>
<td>Specifies the total number of clients managed by the DHCP server.</td>
</tr>
<tr>
<td>Hosts used</td>
<td>Specifies the total number of clients using the IP addresses provided by the DHCP server.</td>
</tr>
<tr>
<td>Hosts unused</td>
<td>Specifies the total number of clients managed by the DHCP server which are not being used.</td>
</tr>
<tr>
<td>Hosts Pending</td>
<td>Specifies the total number of DHCP IP address requests which are pending by the DHCP server.</td>
</tr>
<tr>
<td>Hosts unavailable</td>
<td>Specifies the total number of DHCP hosts which are unavailable i.e; whose lease period have expired.</td>
</tr>
</tbody>
</table>
### Static DHCP
Denotes statistical information about the hosts configured with Static DHCP.

### Automatic DHCP
Denotes statistical information about the hosts configured with Automatic DHCP.

### Static BootP
Denotes statistical information about the hosts configured under Static BootP. **Note:** BootP Relay is disabled when DHCP server is enabled on the switch.

### Automatic BootP
Denotes statistical information about the hosts configured with Automatic BootP.

### Subnet statistics
Denotes all DHCP related statistical information for individual subnets.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range</td>
<td>Specifies the range of IP addresses in the individual subnet.</td>
</tr>
<tr>
<td>Mask</td>
<td>Specifies the subnet mask.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the type of IP address allocation is dynamic or static.</td>
</tr>
</tbody>
</table>

### Release History
Release 7.3.4; command introduced.

### Related Commands
- **clear dhcp-server statistics** Clears the DHCP Server lease statistics.

### MIB Objects

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
clear dhcp-server statistics

Clears the packet counters of DHCP server statistics.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to clear the packet counters of DHCP server statistics.

**Examples**

-> clear dhcp-server statistics

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `show dhcp-server statistics`  
  Displays the DHCP Server lease statistics.

**MIB Objects**

N/A
dhcpv6-server

Enables or disables the DHCPv6 server operation.

```
dhcpv6-server {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the DHCPv6 server.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the DHCPv6 server.</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The dhcpdv6.conf and dhcpdv6.pcy files will be parsed when the DHCPv6 status is enabled for the first time.
- There will be one instance of DHCPv6 for the default VRF.

**Examples**

```
-> dhcpv6-server enable
-> dhcpv6-server disable
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- **show dhcpv6-server leases**  Displays the leases offered by the DHCPv6 server.
- **dhcpv6-server restart**  Allows to restart the DHCPv6 server when the dhcpdv6.conf or dhcpdv6.pcy file is modified.
- **clear dhcpv6-server statistics**  Displays the statistics of the DHCPv6 server.

MIB Objects

- **alaDhcpv6SrvGlobalConfigStatus**
**dhcpv6-server restart**

Allows to restart the DHCPv6 server when the dhcpdv6.conf or dhcpdv6.pcy file is modified.

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> dhcpv6-server restart

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

`dhcpv6-server` Enables or disables the DHCPv6 server operation.

**MIB Objects**

alaDhcpv6SrvGlobalRestart
show dhcpv6-server leases

Displays the leases offered by the DHCPv6 server.

show dhcpv6-server leases [ip-address ipv6_address | type {static | dynamic}] [count]

**Syntax Definitions**

- `ipv6_address`: Specifies IPv6 address of the interface configured with DHCPv6 server.
- `static`: Displays only static leases.
- `dynamic`: Displays only dynamic leases.
- `count`: Count of DHCPv6 messages recorded.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> show dhcpv6-server leases

Total leases: 8

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Lease Granted</th>
<th>Pref Lease Expiry</th>
<th>Valid Lease Expiry</th>
<th>Type</th>
</tr>
</thead>
</table>

-> show dhcpv6-server leases ip-address 2001:100::3

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Lease Granted</th>
<th>Pref Lease Expiry</th>
<th>Valid Lease Expiry</th>
<th>Type</th>
</tr>
</thead>
</table>

-> show dhcpv6-server leases type static

Total leases: 1

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Lease Granted</th>
<th>Pref Lease Expiry</th>
<th>Valid Lease Expiry</th>
<th>Type</th>
</tr>
</thead>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The IP address allocated to the client.</td>
</tr>
<tr>
<td>Lease Granted</td>
<td>The date and time at which lease is granted.</td>
</tr>
<tr>
<td>Pref Lease Expiry</td>
<td>The date and time at which lease expires.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of lease offered.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

*clear dhcpv6-server statistics*  
Clears the DHCPv6 server lease statistics.

**MIB Objects**

alaDhcpv6SrvLeaseTable
  - alaDhcpv6SrvLeaseIpAddress
  - alaDhcpv6SrvLeaseLeaseGrant
  - alaDhcpv6SrvLeaseLeaseExpiry
  - alaDhcpv6SrvLeaseType
show dhcpv6-server statistics

Displays the statistics of the DHCPv6 server.

show dhcpv6-server statistics [packets | hosts | subnets | all]

Syntax Definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>packets</td>
<td>Displays general statistical information along with specific information about data packets received, dropped, and transmitted.</td>
</tr>
<tr>
<td>hosts</td>
<td>Displays general statistical information along with specific information about leases related to the DHCPv6 server.</td>
</tr>
<tr>
<td>subnets</td>
<td>Displays general statistical information along with specific information about all the subnets.</td>
</tr>
<tr>
<td>all</td>
<td>Displays all statistical information related to the DHCPv6 server.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

DHCPv6 server should be enabled before using this command.

Examples

-> show dhcpv6-server statistics
General:
DHCPv6 Server Name : DHCPv6,
DHCPv6 Server Status : Enabled,
Total Subnets Managed : 4,
Total Subnets Used : 0,
Total Subnets Unused : 4,
Total Subnets Full : 0,
DHCPv6 Server System Up Time : Mon Jan 12 05:49:54.198,
Lease DB Sync time (in sec) : 60,
Last sync time : Mon Jan 12 08:41:02 2015,
Next sync time : Mon Jan 12 08:42:02 201

-> show dhcpv6-server statistics packets
Packet:
Total DHCPv6 Solicts          : 0,
Total DHCPv6 Advertises       : 0,
Total DHCPv6 Requests         : 0,
Total DHCPv6 Renews           : 0,
Total DHCPv6 Rebinds          : 0,
Total DHCPv6 Declines         : 0,
Total DHCPv6 Confirms         : 0,
Total DHCPv6 Replies           : 0,
Total DHCPv6 Releases         : 0,
Total DHCPv6 Information Requests : 0,
Total DHCPv6 Lease Queries    : 0,
Total Delete Leases           : 0,
Total Unknown packets         : 0

-> show dhcpv6-server statistics leases
Leases:
  Total:
    Leases Managed : 50190,
    Leases used    : 0,
    Leases unused  : 50190,
    Leases Pending : 0,
    Leases unavailable : 0
Static DHCPv6:
    Leases Managed : 10,
    Leases used    : 0,
    Leases unused  : 10,
    Leases Pending : 0,
    Leases unavailable : 0
Dynamic DHCPv6:
    Leases Managed : 50180,
    Leases used    : 0,
    Leases unused  : 50180,
    Leases Pending : 0,
    Leases unavailable : 0

-> show dhcpv6-server statistics subnets
Subnets:
  Subnet 1:
    SubnetAddr : 2620:0:60:1480::,
    Total       : 17666,
    Static DHCP  : 1,
    Dynamic DHCP : 17665,
Ranges:
  Range1:
    Start             : 2620:0:60:1480::1f01,
    End               : 2620:0:60:1480::1f01,
    PrefixLength      : 97,
    Type               : 1,
    inUse              : 0,
    Unused             : 1,
    Pending            : 0,
    Unavailable        : 0
  Range2:
    Start             : 2620:0:60:1480::2000,
    End               : 2620:0:60:1480::6500,
    PrefixLength      : 97,
    Type               : 2,
    inUse              : 0,
    Unused             : 17665,
Pending              : 0,
Unavailable           : 0

Subnet 2:

SubnetAddr      : 2620:0:60:1481::,
Total           : 29956,
Static DHCP     : 3,
Dynamic DHCP    : 29953,
Ranges:
  Range1:
    Start                 : 2620:0:60:1481::1f01,
    End                   : 2620:0:60:1481::1f01,
    PrefixLength          : 64,
    Type                  : 1,
    inUse                 : 0,
    Unused                : 1,
    Pending               : 0,
    Unavailable           : 0
  Range2:
    Start                 : 2620:0:60:1481::1f02,
    End                   : 2620:0:60:1481::1f02,
    PrefixLength          : 64,
    Type                  : 1,
    inUse                 : 0,
    Unused                : 1,
    Pending               : 0,
    Unavailable           : 0
  Range3:
    Start                 : 2620:0:60:1481::1f03,
    End                   : 2620:0:60:1481::1f03,
    PrefixLength          : 64,
    Type                  : 1,
    inUse                 : 0,
    Unused                : 1,
    Pending               : 0,
    Unavailable           : 0
  Range4:
    Start                 : 2620:0:60:1481::2000,
    End                   : 2620:0:60:1481::9500,
    PrefixLength          : 64,
    Type                  : 2,
    inUse                 : 0,
    Unused                : 29953,
    Pending               : 0,
    Unavailable           : 0

Subnet 3:

SubnetAddr      : 2620:0:60:1482::,
Total           : 1284,
Static DHCP     : 3,
Dynamic DHCP    : 1281,
Ranges:
  Range1:
    Start                 : 2620:0:60:1482::1f01,
    End                   : 2620:0:60:1482::1f01,
    PrefixLength          : 64,
    Type                  : 1,
    inUse                 : 0,
    Unused                : 1,
    Pending               : 0,
    Unavailable           : 0
DHCP Relay Commands

show dhcpv6-server statistics

Range2:
Start : 2620:0:60:1482::1f02,
End : 2620:0:60:1482::1f02,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0

Range3:
Start : 2620:0:60:1482::1f03,
End : 2620:0:60:1482::1f03,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0

Range4:
Start : 2620:0:60:1482::3000,
End : 2620:0:60:1482::3500,
PrefixLength : 64,
Type : 2,
inUse : 0,
Unused : 1281,
Pending : 0,
Unavailable : 0

Subnet 4:
SubnetAddr : 2620:0:60:1483::,
Total : 1284,
Static DHCP : 3,
Dynamic DHCP : 1281,
Ranges:
Range1:
Start : 2620:0:60:1483::1f01,
End : 2620:0:60:1483::1f01,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0

Range2:
Start : 2620:0:60:1483::1f02,
End : 2620:0:60:1483::1f02,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0

Range3:
Start : 2620:0:60:1483::1f03,
End : 2620:0:60:1483::1f03,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
DHCPv6 Server Statistics

Unavailable : 0
Range4:
Start : 2620:0:60:1483::4000,
End : 2620:0:60:1483::4500,
PrefixLength : 64,
Type : 2,
inUse : 0,
Unused : 1281,
Pending : 0,
Unavailable : 0

-> show dhcpv6-server statistics all

General:
DHCPv6 Server Name : DHCPv6,
DHCPv6 Server Status : Enabled,
Total Subnets Managed : 4,
Total Subnets Used : 0,
Total Subnets Unused : 4,
Total Subnets Full : 0,
DHCPv6 Server System Up Time : Mon Jan 12 05:49:54.198,
  Lease DB Sync time (in sec) : 60,
  Last sync time : Mon Jan 12 08:45:02 2015,
  Next sync time : Mon Jan 12 08:46:02 2015
Packet:
Total DHCPv6 Solicts : 0,
Total DHCPv6 Advertises : 0,
Total DHCPv6 Requests : 0,
Total DHCPv6 Renews : 0,
Total DHCPv6 Rebinds : 0,
Total DHCPv6 Declines : 0,
Total DHCPv6 Confirms : 0,
Total DHCPv6 Replys : 0,
Total DHCPv6 Releases : 0,
Total DHCPv6 Information Requests : 0,
Total DHCPv6 Lease Queries : 0,
Total Delete Leases : 0,
Total Unknown packets : 0
Leases:
  Total:
  Leases Managed : 50190,
  Leases used : 0,
  Leases unused : 50190,
  Leases Pending : 0,
  Leases unavailable : 0
Static DHCPv6:
  Leases Managed : 10,
  Leases used : 0,
  Leases unused : 10,
  Leases Pending : 0,
  Leases unavailable : 0
Dynamic DHCPv6:
  Leases Managed : 50180,
  Leases used : 0,
  Leases unused : 50180,
  Leases Pending : 0,
  Leases unavailable : 0
Subnets:
  Subnet 1:
    SubnetAddr : 2620:0:60:1480::,
DHCP Relay Commands

```
Total           : 17666,
Static DHCP     : 1,
Dynamic DHCP    : 17665,
Ranges:
 Range1:
   Start                 : 2620:0:60:1480::1f01,
   End                   : 2620:0:60:1480::1f01,
   PrefixLength          : 97,
   Type                  : 1,
   inUse                 : 0,
   Unused                : 1,
   Pending               : 0,
   Unavailable           : 0
 Range2:
   Start                 : 2620:0:60:1480::2000,
   End                   : 2620:0:60:1480::6500,
   PrefixLength          : 97,
   Type                  : 2,
   inUse                 : 0,
   Unused                : 17665,
   Pending               : 0,
   Unavailable           : 0
Subnet 2:
 SubnetAddr      : 2620:0:60:1481::,
Total           : 29956,
Static DHCP     : 3,
Dynamic DHCP    : 29953,
Ranges:
 Range1:
   Start                 : 2620:0:60:1481::1f01,
   End                   : 2620:0:60:1481::1f01,
   PrefixLength          : 64,
   Type                  : 1,
   inUse                 : 0,
   Unused                : 1,
   Pending               : 0,
   Unavailable           : 0
 Range2:
   Start                 : 2620:0:60:1481::1f02,
   End                   : 2620:0:60:1481::1f02,
   PrefixLength          : 64,
   Type                  : 1,
   inUse                 : 0,
   Unused                : 1,
   Pending               : 0,
   Unavailable           : 0
 Range3:
   Start                 : 2620:0:60:1481::1f03,
   End                   : 2620:0:60:1481::1f03,
   PrefixLength          : 64,
   Type                  : 1,
   inUse                 : 0,
   Unused                : 1,
   Pending               : 0,
   Unavailable           : 0
 Range4:
   Start                 : 2620:0:60:1481::2000,
   End                   : 2620:0:60:1481::9500,
   PrefixLength          : 64,
```
DHCP Relay Commands

Type : 2,
inUse : 0,
Unused : 29953,
Pending : 0,
Unavailable : 0

Subnet 3:
SubnetAddr : 2620:0:60:1482::,
Total : 1284,
Static DHCP : 3,
Dynamic DHCP : 1281,
Ranges:
Range1:
Start : 2620:0:60:1482::1f01,
End : 2620:0:60:1482::1f01,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0
Range2:
Start : 2620:0:60:1482::1f02,
End : 2620:0:60:1482::1f02,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0
Range3:
Start : 2620:0:60:1482::1f03,
End : 2620:0:60:1482::1f03,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0
Range4:
Start : 2620:0:60:1482::3000,
End : 2620:0:60:1482::3500,
PrefixLength : 64,
Type : 2,
inUse : 0,
Unused : 1281,
Pending : 0,
Unavailable : 0

Subnet 4:
SubnetAddr : 2620:0:60:1483::,
Total : 1284,
Static DHCP : 3,
Dynamic DHCP : 1281,
Ranges:
Range1:
Start : 2620:0:60:1483::1f01,
DHCP Relay Commands

show dhcpv6-server statistics

Unused : 1,
Pending : 0,
Unavailable : 0

Range2:
Start : 2620:0:60:1483::1f02,
End : 2620:0:60:1483::1f02,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0

Range3:
Start : 2620:0:60:1483::1f03,
End : 2620:0:60:1483::1f03,
PrefixLength : 64,
Type : 1,
inUse : 0,
Unused : 1,
Pending : 0,
Unavailable : 0

Range4:
Start : 2620:0:60:1483::4000,
End : 2620:0:60:1483::4500,
PrefixLength : 64,
Type : 2,
inUse : 0,
Unused : 1281,
Pending : 0,
Unavailable : 0

output definitions

General
Denotes general DHCPv6 Server statistics.

DHCPv6 Server Name
Specifies the name assigned to the DHCPv6 server.

DHCPv6 Server Status
Specifies up or down status of the DHCPv6 server.

Total subnets used
Specifies the total number of subnets being used.

Total subnets managed
Specifies the total number of subnets being managed by the DHCPv6 server.

Total subnets unused
Specifies the total number of subnets being unused.

Total subnets full
Specifies the total number of subnets where all the IP addresses are used.

DHCP Server System Up Time
Shows the DHCPv6 Server System Up Time Performance Monitor counter.

Sync time
Specifies the time for DHCPv6 server to contact and synchronize with the designated time server.

Last sync time
Specifies the last time the synchronization occurred.

Next sync time
Specifies the next time the synchronization should be scheduled.

Packet stats
Denotes statistical information about the data packet transmission.

Total DHCP Discovers
Specifies the total number of DHCPDISCOVER packets sent by the clients to the DHCPv6 server.
### Output Definitions (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total DHCP Offers</strong></td>
<td>Specifies the total number of DHCPOFFER packets sent by the server to the clients.</td>
</tr>
<tr>
<td><strong>Total DHCP Requests</strong></td>
<td>Specifies the total number of DHCPREQUEST packets sent by the clients in response to the DHCPOFFER packets.</td>
</tr>
<tr>
<td><strong>Total DHCP Request Grants</strong></td>
<td>Specifies the total number of DHCPv6 request grants provided by the server to the clients.</td>
</tr>
<tr>
<td><strong>Total DHCP Request Renews</strong></td>
<td>Specifies the total number of DHCPv6 lease renew requests sent by the clients to the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Total DHCP Declines</strong></td>
<td>Specifies the total number of DHCPv6 requests declined by the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Total DHCP Acks</strong></td>
<td>Specifies the total number of DHCPACK acknowledgement packets sent by the DHCPv6 server to the clients.</td>
</tr>
<tr>
<td><strong>Total DHCP Nacks</strong></td>
<td>Specifies the total number of DHCPv6 Negative acknowledgements sent from the DHCPv6 server to the clients. The DHCPNACK message is sent when all the IP addresses available to the server are exhausted and the client sends a DHCPREQUEST.</td>
</tr>
<tr>
<td><strong>Total DHCP Releases</strong></td>
<td>Specifies the total number of DHCPRELEASE packets sent by the DHCPv6 server to release IP addresses from its clients.</td>
</tr>
<tr>
<td><strong>Total DHCP Informs</strong></td>
<td>Specifies the total number of DHCPINFORM packets sent by the clients to obtain DHCPv6 options from the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Total Bootp requests</strong></td>
<td>Specifies the total number of BOOTP requests sent by the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Total Bootp response</strong></td>
<td>Specifies the total number of BOOTP response packets sent by the DHCPv6 server to the clients.</td>
</tr>
<tr>
<td><strong>Total Unknown packets</strong></td>
<td>Specifies the total number of unknown or badly formatted DHCPv6 packets received by the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Leases stats</strong></td>
<td>Denotes statistical information about leases provided by the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Hosts Managed</strong></td>
<td>Specifies the total number of clients managed by the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Hosts used</strong></td>
<td>Specifies the total number of clients using the IP addresses provided by the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Hosts unused</strong></td>
<td>Specifies the total number of clients managed by the DHCPv6 server which are not being used.</td>
</tr>
<tr>
<td><strong>Hosts Pending</strong></td>
<td>Specifies the total number of DHCPv6 IP address requests which are pending by the DHCPv6 server.</td>
</tr>
<tr>
<td><strong>Hosts unavailable</strong></td>
<td>Specifies the total number of DHCPv6 hosts which are unavailable (for example, hosts whose lease period has expired).</td>
</tr>
<tr>
<td><strong>Static DHCP</strong></td>
<td>Denotes statistical information about the hosts configured with Static DHCPv6.</td>
</tr>
<tr>
<td><strong>Automatic DHCP</strong></td>
<td>Denotes statistical information about the hosts configured with Automatic DHCPv6.</td>
</tr>
</tbody>
</table>
| **Static BootP**               | Denotes statistical information about the hosts configured under Static BootP. **Note:** BootP Relay is disabled when DHCPv6 server is enabled on the switch.
output definitions (continued)

<table>
<thead>
<tr>
<th>Automatic BootP</th>
<th>Denotes statistical information about the hosts configured with Automatic BootP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet statistics</td>
<td>Denotes all DHCPv6 related statistical information for individual subnets.</td>
</tr>
<tr>
<td>Range</td>
<td>Specifies the range of IP addresses in the individual subnet.</td>
</tr>
<tr>
<td>Mask</td>
<td>Specifies the subnet mask.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the type of IP address allocation is dynamic or static.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command introduced.

Related Commands

clear dhcpv6-server statistics  Clears the DHCPv6 Server lease statistics.

MIB Objects

N/A
clear dhcpv6-server statistics

Clears the packet counters of DHCPv6 server statistics.

clear dhcpv6-server statistics

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to clear the packet counters of DHCPv6 server statistics.

**Examples**

`-> clear dhcpv6-server statistics`

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `show dhcpv6-server statistics` Displays the DHCPv6 Server lease statistics.

**MIB Objects**

N/A
**dhcp-message-service**

Enable or disable the message service operation.

```
dhcp-message-service {enable | disable}
```

### Syntax Definitions

- **enable** Enables the operational status of the message service.
- **disable** Disables the operational status of the message service.

### Defaults

By default, the operational status of the message service is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The **conf** and **pcy** files are parsed when message service is enabled.
- There is one instance of the message service for the default VRF in the switch that can be enabled or disabled.

### Examples

```
-> dhcp-message-service enable
-> dhcp-message-service disable
```

### Release History

Release 7.3.4; command introduced.

### Related Commands

- **dhcp-message-service restart** Restarts the message service after the msgd.conf file is modified.

### MIB Objects

- **alaMsgSrvGlobalConfigStatus**

---

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 25-122
**dhcp-message-service restart**

Restarts the message service after the `msgd.conf` file or `dhcpd.pcy` is modified.

`dhcp-message-service restart`

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using this command, enable the message service status using the `dhcp-message-service` command.

**Examples**

```
-> message-service restart
```

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `dhcp-message-service` Enable or disable the message service operation.

**MIB Objects**

- `alaMsgSrvGlobalRestart`
show message-service status

Displays the status and statistical information related to the message service running on the switch.

show message-service status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show message-service status
Message Service is enabled

Release History

Release 7.3.4; command introduced.

Related Commands

dhcp-message-service  Enable or disable the message service operation.
dhcp-message-service restart  Restarts the message service, after the msgd.conf file is modified.

MIB Objects

N/A
**active-lease-service**

Enable or disable the Active Lease Service operation.

`active-lease-service {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the operational status of the Active Lease Service.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the operational status of the Active Lease Service.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, the operational status of Active Lease Service is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>9000 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

There is one instance of Active Lease Service for the default VRF in the switch that can be enabled or disabled.

**Examples**

```
-> active-lease-service enable
-> active-lease-service disable
```

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `active-lease-service restart`: Restarts the Active Lease Service after the netd.pcy file is modified.
- `show active-lease-service status`: Displays the status and statistical information related to Active Lease Service running on the switch.

**MIB Objects**

`alaActiveLeaseSrvGlobalConfigStatus`
**active-lease-service restart**

Restarts the Active Lease Service after the netd.pcy file is modified.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before using this command, enable the Active Lease Service using the `active-lease-service` command.

**Examples**

```
-> active-lease-service restart
```

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `active-lease-service` Enable or disable the Active Lease Service operation.
- `show active-lease-service status` Displays the status and statistical information related to Active Lease Service running on the switch.

**MIB Objects**

- `alaActiveLeaseSrvGlobalRestart`
show active-lease-service status

Displays the status and statistical information related to the Active Lease Service running on the switch.

show active-lease-service status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show active-lease-service status
Active Lease Service is enabled

Release History

Release 7.3.4; command introduced.

Related Commands

active-lease-service    Enable or disable the Active Lease Service operation.

MIB Objects

N/A
**dhcp-snooping admin-state**

Enables or disables DHCP Snooping for the switch.

```
dhcp-snooping admin-state {enable | disable}
```

```
no dhcp-snooping
```

---

**Syntax Definitions**

- **enable**: Enables DHCP Snooping for the switch.
- **disable**: Disables DHCP Snooping for the switch.

**Defaults**

By default, this feature is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When DHCP Snooping is administratively disabled for the switch, the DHCP Snooping configuration remains and dynamic binding table entries are cleared.
- When the `no` form of the command is used, the DHCP Snooping configuration is removed and dynamic binding table entries are cleared.

**Examples**

```
-> dhcp-snooping admin-state enable
-> dhcp-snooping admin-state disable
-> no dhcp-snooping
```

**Release History**

Release 7.3.4; command introduced.
Release 8.6R1; `no` form of the command added.
Related Commands

dhcp-snooping vlan
   Enables or disables DHCP Snooping on a per-VLAN basis.
show dhcp-snooping
   Displays the current DHCP Snooping configuration for the switch.

MIB Objects

dhcpSnoopingMode
**dhcp-snooping mac-address-verification**

Globally enables or disables MAC address verification for incoming DHCP traffic. When this feature is enabled, the source MAC address is compared to the client hardware MAC address in the DHCP packet. If these two addresses do not match, the DHCP packet is dropped.

```
dhcp-snooping mac-address-verification admin-state {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables DHCP MAC address verification for the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables DHCP MAC address verification for the switch.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, this feature is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- DHCP Snooping must be enabled before using this command.

- When DHCP Snooping is enabled at the switch level, MAC address verification and Option-82 data insertion are enabled by default. In addition, the trust mode for all ports is set to the DHCP client only mode.

- Changing the enabled or disabled status for MAC address verification is only allowed when DHCP Snooping is globally enabled for the switch.

**Examples**

```
-> dhcp-snooping mac-address-verification admin-state enable
-> dhcp-snooping mac-address-verification admin-state disable
```

**Release History**

Release 7.3.4; command introduced.
Related Commands

- `dhcp-snooping admin-state` Globally enables or disables DHCP Snooping for the switch.
- `dhcp-snooping option-82-data-insertion` Globally enables or disables DHCP Option-82 data insertion for DHCP packets.
- `show dhcp-snooping` Displays the current DHCP Snooping configuration for the switch.

MIB Objects

- `dhcpSnoopingMacAddrVerificationStatus`
**dhcp-snooping option-82-data-insertion**

Globally enables or disables DHCP Option-82 data insertion for DHCP packets. When this feature is enabled, the relay agent inserts the Option-82 field into DHCP packets before forwarding them to the DHCP server.

**dhcp-snooping option-82-data-insertion admin-state {enable | disable}**

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables inserting the DHCP Option-82 field into DHCP packets.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables inserting the DHCP Option-82 field into DHCP packets.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, this feature is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td>Yes</td>
</tr>
<tr>
<td>9900 X32E/T24C2/ X24C2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- DHCP Snooping must be enabled before using this command.
- When DHCP Snooping is enabled at the switch level, Option-82-data-insertion and MAC address verification are enabled by default. In addition, the trust mode for all ports is set to the DHCP client only mode.

**Examples**

- `-> dhcp-snooping option-82-data-insertion admin-state enable`
- `-> dhcp-snooping option-82-data-insertion admin-state disable`

**Release History**

Release 7.3.4; command introduced.
**Related Commands**

- **dhcp-snooping admin-state**: Globally enables or disables DHCP Snooping for the switch.
- **dhcp-snooping option-82 format**: Configures the type of information that is inserted in both the Circuit ID and Remote ID suboption of the Option-82 field.
- **show dhcp-snooping**: Displays the current DHCP Snooping configuration for the switch.

**MIB Objects**

- `dhcpSnoopingOpt82DataInsertionStatus`
**dhcp-snooping bypass option-82-check**

Enables or disables checking for an Option-82 field in DHCP packets ingressing on untrusted ports.

```
dhcp-snooping bypass option-82-check admin-state {enable | disable}
```

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Bypasses the Option-82 field check.</td>
</tr>
<tr>
<td>disable</td>
<td>Checks DHCP packets for the Option-82 field.</td>
</tr>
</tbody>
</table>

---

**Defaults**

By default, this feature is disabled.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- When this feature is disabled (the default), DHCP packets ingressing on untrusted ports are checked to see if they contain the Option-82 field. If this field is present, the DHCP packet is discarded.

- When this feature is enabled, DHCP packets ingressing on untrusted ports are not checked to see if they contain the Option-82 field. In this case, the Option-82 field is ignored and all DHCP packets are processed.

- Using this command is only allowed when DHCP Snooping is enabled globally for the switch or at the VLAN level.

---

**Examples**

```
-> dhcp-snooping bypass option-82-check admin-state enable
-> dhcp-snooping bypass option-82-check admin-state disable
```

---

**Release History**

Release 7.3.4; command introduced.
Related Commands

- **dhcp-snooping admin-state**: Globally enables or disables DHCP Snooping for the switch.
- **show dhcp-snooping**: Displays the current DHCP Snooping configuration for the switch.

MIB Objects

- **dhcpSnoopingBypassOpt82CheckStatus**
**dhcp-snooping option-82 format**

Configures the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 field.

**Dhcp-snooping option-82 format [base-mac | system-name | user-string string | interface-alias | auto-interface-alias | ascii] { remote-id | circuit-id} [base-mac | cvlan | interface | interface-alias | system-name | user-string string | vlan} {delimiter string}]

**no dhcp-snooping option-82 format ascii {remote-id | circuit-id}**

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-mac</td>
<td>The base MAC address of the switch.</td>
</tr>
<tr>
<td>system-name</td>
<td>The system name of the switch.</td>
</tr>
<tr>
<td>string</td>
<td>A user defined text string. Supports up to 64 characters.</td>
</tr>
<tr>
<td>interface-alias</td>
<td>The alias configured for the interface.</td>
</tr>
<tr>
<td>auto-interface-alias</td>
<td>The switch automatically generates the interface-alias in the following format: SystemName_slot_port. ascii ASCII format.</td>
</tr>
<tr>
<td>ascii</td>
<td>ASCII format.</td>
</tr>
<tr>
<td>remote-id</td>
<td>Select the sub-id fields of option-82 to configure ASCII.</td>
</tr>
<tr>
<td>circuit-id</td>
<td>Select the sub-id fields of option-82 to configure ASCII.</td>
</tr>
<tr>
<td>base-mac</td>
<td>The base MAC address of the switch.</td>
</tr>
<tr>
<td>cvlan</td>
<td>The Customer VLAN ID.</td>
</tr>
<tr>
<td>interface</td>
<td>The interface name.</td>
</tr>
<tr>
<td>interface-alias</td>
<td>The alias configured for the interface.</td>
</tr>
<tr>
<td>system-name</td>
<td>The system name of the switch.</td>
</tr>
<tr>
<td>user-string</td>
<td>A user defined text string.</td>
</tr>
<tr>
<td>vlan</td>
<td>The VLAN ID of which the client is a member.</td>
</tr>
<tr>
<td>string</td>
<td>A user-defined text string.</td>
</tr>
<tr>
<td>delimiter</td>
<td>The delimiter character that separates fields within the Circuit ID and Remote ID ASCII string value. Valid characters are</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-string</td>
<td>base-mac</td>
</tr>
<tr>
<td>system-name</td>
<td>base-mac</td>
</tr>
<tr>
<td>interface-alias</td>
<td>base-mac</td>
</tr>
<tr>
<td>auto-interface-alias</td>
<td>ascii base-mac</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The string parameter specifies user-defined information to insert into the Circuit ID and Remote ID fields.

- When entering a string for user-defined Option-82 information, quotes are required around ambiguous characters, such as hex characters, spaces, etc, so they are interpreted as text. For example, the string “Building B Server” requires quotes because of the spaces between the words.

- The interface-alias parameter will use the alias configured with the interfaces alias command. If no alias is configured a NULL string will be inserted.

- A maximum of 63 characters can be inserted when using the interface-alias and auto-interface-alias commands, remaining characters will be truncated.

- The Option-82 format option is a global setting, the format specified will be applied to all ports on the switch.

- The data specified with this command is added to the Circuit ID and Remote ID fields only when DHCP Option-82 data insertion is enabled for the switch.

- When DHCP Snooping is enabled at the switch level, Option-82 data insertion is enabled by default.

- The ASCII option is used to specify the type of information that is configured in ASCII text string format and then inserted into the Option-82 Circuit ID suboption. Each parameter provided with this command represents a different type of information.

- Configuring the Circuit ID or Remote ID suboption in ASCII format allows up to five fields (types) of information within the ASCII string. However, if the contents of all the fields combined exceeds 127 characters, then the ASCII string is truncated.

- Specifying at least one parameter with ASCII option is required. If multiple parameters are selected, then specifying one of the valid delimiter characters is also required.

- In order for the backward slash “\” delimiter to be parsed correctly it must be entered as “\\”.

- Use the no form of this command to remove the type of information that is inserted into both the Circuit ID and Remote ID suboption fields of the Option-82 fields option-82-check admin-state disable.

Examples

- `-> dhcp-snooping option-82 format user-string “Building B Server”`
- `-> dhcp-snooping option-82 format system-name`
- `-> dhcp-snooping option-82 format base-mac`
- `-> dhcp-snooping option-82 format interface-alias`
- `-> dhcp-snooping option-82 format auto-interface-alias`
-> no dhcp-snooping option-82 format ascii remote-id
-> no dhcp-snooping option-82 format ascii circuit-id
-> dhcp-snooping option-82 format ascii circuit-id cvlan cvlan delimiter "\\"

Release History
Release 7.3.4; command introduced.

Related Commands

dhcp-snooping option-82-data-insertion  Globally enables or disables DHCP Option-82 data insertion for DHCP packets.
dhcp-snooping admin-state     Globally enables or disables DHCP Snooping for the switch
show dhcp-snooping            Displays the current DHCP Snooping configuration for the switch.

MIB Objects

  dhcpSnoopingOption82FormatType
  dhcpSnoopingOption82StringValue
  dhcpSnoopingOption82FormatASCIIConfigurableEntry
  dhcpSnoopingOption82FormatASCIIConfigurableIndex
  dhcpSnoopingOption82FormatASCIIConfigurableField1
  dhcpSnoopingOption82FormatASCIIConfigurableField2
  dhcpSnoopingOption82FormatASCIIConfigurableField3
  dhcpSnoopingOption82FormatASCIIConfigurableField4
  dhcpSnoopingOption82FormatASCIIConfigurableField5
  dhcpSnoopingOption82FormatASCIIConfigurableDelimiter
**dhcp-snooping option-82 policy**

Specifies whether to keep, replace, or drop the Option-82 field from DHCP packets entering the switch.

`dhcp-snooping option-82 policy [replace | keep | drop]`

### Syntax Definitions

- **replace**: Replaces Option-82 field in the incoming DHCP packets.
- **keep**: Keeps Option-82 field in the incoming DHCP packets.
- **drop**: Drops the packet with Option-82 in the incoming DHCP packets.

### Defaults

By default, the Option-82 field is replaced in the DHCP packets.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

-> dhcp-snooping option-82 policy replace
-> dhcp-snooping option-82 policy keep
-> dhcp-snooping option-82 policy drop

### Release History

Release 8.5R2; command introduced.

### Related Commands

- **dhcp-snooping admin-state**: Globally enables or disables DHCP Snooping for the switch.
- **show dhcp-snooping**: Displays the global DHCP Snooping configuration.

### MIB Objects

- `dhcpSnoopingOption82Policy`
dhcp-snooping vlan

Enables or disables DHCP Snooping on a per VLAN basis. When this feature is enabled, all DHCP packets received on ports associated with the DHCP Snooping VLAN are filtered.

```
dhcp-snooping vlan vlan_id[-vlan_id2] [mac-address-verification | option-82-data-insertion] admin-state {enable | disable}
```

```
no dhcp-snooping vlan vlan_id[-vlan_id2]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`: The VLAN identification number. Valid range is 1–4094. Use a hyphen to specify a range of VLANs (10-15).
- `mac-address verification`: Enables or disables verifying the source MAC address of DHCP packets with the client MAC address contained in the same packet.
- `option-82 data-insertion`: Enables or disables inserting Option-82 information into DHCP packets.
- `admin-state`: Enables or disables DHCP snooping feature for specified VLAN.

**Defaults**

By default, DHCP Snooping is disabled. When this feature is enabled for the specified VLAN, the following default parameter values apply:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address verification</td>
<td>Enabled</td>
</tr>
<tr>
<td>option-82 data-insertion</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the DHCP Snooping configuration for the specified VLAN.
- The MAC address verification and Option-82 data insertion are applied to packets received on ports associated with the DHCP Snooping VLAN.
If the DHCP relay agent Option-82 feature is enabled, DHCP Snooping is not available. These two features are mutually exclusive.

If the DHCP Snooping feature is globally enabled for the switch, then configuring snooping on a per-VLAN basis is not allowed. The opposite is also true; invoking VLAN based snooping prevents the use of switch level snooping.

Note that disabling the DHCP Snooping Option-82 data insertion operation for a VLAN is not allowed when the binding table functionality is enabled.

Examples

- `dhcp-snooping vlan 100 admin-state enable`
- `dhcp-snooping vlan 100 admin-state disable`
- `dhcp-snooping vlan 100 mac-address-verification admin-state enable`
- `no dhcp-snooping vlan 100`
- `dhcp-snooping vlan 200-205 admin-state enable`
- `dhcp-snooping vlan 200-205 admin-state disable`
- `dhcp-snooping vlan 200-205 option-82 data-insertion admin-state enable`
- `no dhcp-snooping vlan 200-205`

Release History

Release 7.3.4; command introduced.
Release 8.6R1; no form of the command added.

Related Commands

- `dhcp-snooping admin-state` Globally enables or disables DHCP Snooping for the switch.
- `show dhcp-snooping vlan` Displays a list of DHCP Snooping VLANs.

MIB Objects

- `dhcpSnoopingVlanTable`
- `dhcpSnoopingVlanNumber`
- `dhcpSnoopingVlanMacAddrVerificationStatus`
- `dhcpSnoopingVlanOpt82DataInsertionStatus`
- `dhcpSnoopingVlanStatus`
- `dhcpSnoopingVlanAdminState`
**dhcp-snooping port**

Configures the DHCP Snooping trust mode for the port. The trust mode determines if the port will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

```
dhcp-snooping port chassis/slot1/port[-port2] {block | client-only | trust}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot1/port[-port2]**: The slot and port number (1/1/3). Use a hyphen to specify a range of ports (1/1/3-8).
- **block**: Blocks all DHCP traffic on the port.
- **client-only**: Allows only DHCP client traffic on the port.
- **trust**: Allows all DHCP traffic on the port. The port behaves as if DHCP Snooping was not enabled.

### Defaults

By default, the trust mode for a port is set to **client-only** when the DHCP Snooping feature is enabled for the switch or for a VLAN.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The DHCP trust mode only applies when the DHCP Snooping feature is enabled for the switch or for a VLAN.
- If DHCP Snooping is enabled at the switch level, the trust mode applies to all switch ports.
- If DHCP Snooping is enabled for a specific VLAN, then the trust mode applies to only those ports that are associated with that VLAN.

### Examples

```
-> dhcp-snooping port 1/1/24 trust
-> dhcp-snooping port 1/1-10 block
-> dhcp-snooping port 1/1/8 client-only
```
**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- **dhcp-snooping admin-state** Globally enables or disables DHCP Snooping for the switch.
- **dhcp-snooping vlan** Enables or disables DHCP Snooping on a per-VLAN basis.
- **show dhcp-snooping port** Displays the current trust mode for a port and statistics regarding the number of packets dropped due to DHCP Snooping violations

**MIB Objects**

- dhcpSnoopingPortTable
  - dhcpSnoopingPortIfIndex
  - dhcpSnoopingPortTrustMode
**dhcp-snooping linkagg**

Configures the DHCP Snooping trust mode for the link aggregate. The trust mode determines if the link aggregate will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

```
dhcp-snooping linkagg agg_id[-agg_id2] {block | client-only | trust}
```

### Syntax Definitions

- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (1-5).
- **block**: Blocks all DHCP traffic on the link aggregate.
- **client-only**: Allows only DHCP client traffic on the link aggregate.
- **trust**: Allows all DHCP traffic on the link aggregate. The link aggregate behaves as if DHCP Snooping was not enabled.

### Defaults

By default, the trust mode for a link aggregate is set to **client-only** when the DHCP Snooping feature is enabled for the switch or for a VLAN.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The DHCP trust mode only applies when the DHCP Snooping feature is enabled for the switch or for a VLAN.
- If DHCP Snooping is enabled at the switch level, the trust mode applies to all link aggregates.
- If DHCP Snooping is enabled for a specific VLAN, then the trust mode applies to only those link aggregates that are associated with that VLAN.
- Use the `show dhcp-snooping port` command to display the current trust mode for a link aggregate and statistics regarding the number of packets dropped due to DHCP Snooping violations.

### Examples

- `-> dhcp-snooping linkagg 1 trust`
- `-> dhcp-snooping linkagg 5-8 trust`
- `-> dhcp-snooping linkagg 2 block`
- `-> dhcp-snooping linkagg 5-8 block`
- `-> dhcp-snooping linkagg 3 client-only`
-> dhcp-snooping linkagg 5-8 client-only

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- **dhcp-snooping admin-state**  Globally enables or disables DHCP Snooping for the switch.
- **dhcp-snooping vlan**  Enables or disables DHCP Snooping on a per-VLAN basis.

**MIB Objects**

dhcpSnoopingPortTable
  
  - dhcpSnoopingPortIfIndex
  - dhcpSnoopingPortTrustMode
**dhcp-snooping ip-source-filter admin-state**

Enables or disables the DHCP Snooping IP source filtering functionality for the switch.

`dhcp-snooping ip-source-filter admin-state {enable | disable}`

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables IP source filtering for the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables IP source filtering for the switch.</td>
</tr>
</tbody>
</table>

### Defaults

By default, the DHCP Snooping IP source filtering functionality is enabled for the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When IP source filtering is disabled for the switch, the user-defined IP source filtering configuration is maintained but not operationally active.
- When DHCP Snooping is disabled for the switch, the status of IP source filtering is not changed; if IP source filtering is enabled, the functionality is still applied to static binding table entries.

### Examples

- `-> dhcp-snooping ip-source-filter admin-state disable`
- `-> dhcp-snooping ip-source-filter admin-state enable`

### Release History

Release 8.6R1; command introduced.

### Related Commands

- **dhcp-snooping ip-source-filter**  Enables or disables DHCP Snooping IP source filtering for a port, link aggregate, or VLAN.
- **show dhcp-snooping ip-source-filter**  Displays the global IP source filtering status.
MIB Objects

dhcpSnoopingIpSourceFilterAdminState
**dhcp-snooping ip-source-filter**

Enables or disables the IP source filtering capability on a port, link aggregate, or VLAN. When this function is enabled, the switch allows the traffic that matches the client IP address, MAC address, port, and VLAN combination obtained from the DHCP snooping binding table entry.

```
dhcp-snooping ip-source-filter {vlan vlan_id|-vlan_id2} [port chassis/slot/port|-port] | linkagg agg_id|-agg_id2] admin-state {enable | disable}
```

**Syntax Definitions**

- `vlan vlan_id|-vlan_id2` The VLAN identification number (1–4094). Use a hyphen to specify a range of VLANs (10-15).
- `chassis` The chassis identifier.
- `slot1/port|-port2` The slot and port number (1/1/3). Use a hyphen to specify a range of ports (1/1/3-8).
- `agg_id|-agg_id2` The link aggregate ID number. Use a hyphen to specify a range of IDs (1-5).
- `enable` Enables IP source filtering for the specified port, link aggregate, or VLAN.
- `disable` Disables IP source filtering for the specified port, link aggregate, or VLAN.

**Defaults**

By default, IP source filtering is disabled for a port, link aggregate, or VLAN.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Source filtering can be enabled only on the VLANs on which the DHCP Snooping is enabled.
- Source filtering can be enabled as follows:
  - on the ports that are associated with a VLAN on which DHCP Snooping is enabled.
  - on all the ports when DHCP Snooping is globally enabled for the switch.
- The user-defined IP source filtering configuration is not operationally active unless the IP source filtering functionality is globally enabled for the switch. By default, the global functionality is enabled and is configurable through the `dhcp-snooping ip-source-filter admin-state` command.
**Examples**

-> dhcp-snooping ip-source-filter port 1/1/1 admin-state enable
-> dhcp-snooping ip-source-filter port 1/1/1-5 admin-state enable
-> dhcp-snooping ip-source-filter linkagg 2 admin-state enable
-> dhcp-snooping ip-source-filter vlan 10 admin-state enable
-> dhcp-snooping ip-source-filter vlan 20 admin-state disable

**Release History**

Release 7.3.4; command introduced.
Release 8.5R2; support for port ranges added.

**Related Commands**

- `dhcp-snooping ip-source-filter admin-state` Enables or disables DHCP Snooping IP source filtering functionality for the switch.
- `show dhcp-snooping ip-source-filter` Displays the ports or VLANs on which IP source filtering is enabled.

**MIB Objects**

- `dhcpSnoopingSourceFilterVlanTable`
  - `dhcpSnoopingSourceFilterVlanNumber`
  - `dhcpSnoopingSourceFilterVlanFilteringStatus`

- `dhcpSnoopingPortTable`
  - `dhcpSnoopingPortIpSourceFiltering`
dhcp-snooping binding admin-state

Enables or disables the DHCP Snooping binding table functionality. The binding table contains the MAC address, IP address, lease time, binding type (dynamic or static), VLAN number, and the interface information that corresponds to a local untrusted port on the switch.

**dhcp-snooping binding admin-state {enable | disable}**

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the creation of binding table entries.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the creation of binding table entries.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, the binding table functionality is enabled when the DHCP Snooping feature is enabled for the switch or for a VLAN.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/X48C8/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Note that enabling the binding table functionality is not allowed if Option-82 data insertion is *not* enabled at either the switch or VLAN level.

**Examples**

- `-> dhcp-snooping binding admin-state disable`
- `-> dhcp-snooping binding admin-state enable`

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- **dhcp-snooping binding timeout** Configures the amount of time between each automatic save of the binding table contents to a file on the switch.
- **dhcp-snooping binding action** Synchronizes the contents of the DHCP Snooping binding table with the contents of the `dhcpBinding.db` file saved on the switch.

**MIB Objects**
dhcpSnoopingBindingStatus
**dhcp-snooping binding timeout**

Configures the amount of time between each automatic save of the DHCP Snooping binding table contents maintained in memory to a file on the switch. This functionality preserves binding table contents across switch reboots.

**dhcp-snooping binding timeout seconds**

---

**Syntax Definitions**

seconds The number of seconds to wait before the next save. The valid range is 1–600.

**Defaults**

By default, the timeout value is set to 1 second.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The timeout value is only valid if the DHCP Snooping binding table functionality is enabled.
- The contents of the binding table is saved to the `dhcpBinding.db` file in the `/flash/switch` directory.
- The `dhcpBinding.db` file is time stamped when a save of the binding table contents is successfully completed.

**Examples**

- `dhcp-snooping binding timeout 600`
- `dhcp-snooping binding timeout 250`

**Release History**

Release 7.3.4; command introduced.
Release 8.6R1; default timeout changed to 1 second and valid timeout range changed to 1–600 seconds.
Related Commands

- **dhcp-snooping binding admin-state**
  Enables or disables the DHCP Snooping binding table functionality.

- **dhcp-snooping binding action**
  Synchronizes the contents of the DHCP Snooping binding table with the contents of the `dhcpBinding.db` file saved on the switch.

MIB Objects

- `dhcpSnoopingBindingDatabaseSyncTimeout`
dhcp-snooping binding action

Triggers a purge, renew, or save action against the DHCP Snooping binding table. A purge action clears the contents of the table. A renew action populates the table with entries saved in the dhcpBinding.db file. A save action saves table entries in switch memory to the dhcpBinding.db file.

**Syntax Definitions**

```
dhcp-snooping binding action {purge | renew | save}
```

**purge**
Clears all binding table entries that are maintained in switch memory.

**renew**
Populates the binding table with entries saved in the dhcpBinding.db file located in the /flash/switch directory on the switch.

**save**
Saves the binding table entries in switch memory to the dhcpBinding.db file located in the /flash/switch directory on the switch.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The DHCP Snooping binding table is maintained in the switch memory. Binding table entries are saved on a periodic basis to the dhcpBinding.db file on the switch. Use the save option to invoke an explicit save of binding table entries to the dhcpBinding.db file.
- To sync the binding table contents with the contents of the dhcpBinding.db file:
  - use the purge option to clear the binding table entries, then
  - use the renew option to repopulate the binding table with entries saved in the dhcpBinding.db file.

**Examples**

- `-> dhcp-snooping binding action purge`
- `-> dhcp-snooping binding action renew`
- `-> dhcp-snooping binding action save`


**Release History**

Release 7.3.4; command introduced.
Release 8.6.R1; `save` option added.

**Related Commands**

- `dhcp-snooping binding admin-state`: Enables or disables the DHCP Snooping binding table functionality.
- `dhcp-snooping binding timeout`: Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

**MIB Objects**

- `dhcpSnoopingBindingDatabaseAction`
**dhcp-snooping binding persistency**

Retains the entries in the DHCP Snooping binding table for the duration of the lease regardless of the existence of the MAC address in the MAC address table.

```
dhcp-snooping binding persistency admin-state {enable | disable}
```

**Syntax Definitions**

- **enable**: Enables DHCP Snooping binding persistency.
- **disable**: Disables DHCP Snooping binding persistency.

**Defaults**

By default, DHCP Snooping binding persistency is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- With this option disabled, the entry will be removed if the MAC address is missing from the MAC address table when the database is synchronized.
- Use the `show dhcp-snooping` command to display the current status.

**Examples**

```
-> dhcp-snooping binding persistency admin-state enable
-> dhcp-snooping binding persistency admin-state disable
```

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `dhcp-snooping binding admin-state`: Enables or disables the DHCP Snooping binding table functionality.
- `dhcp-snooping binding timeout`: Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

**MIB Objects**
dhcpSnoopingBindingPersistencyStatus
**dhcp-snooping binding**

Creates a static entry in the binding table.

```
dhcp-snooping binding mac_address port chassis/slot/port address ip_address vlan vlan_id
```

```
no dhcp-snooping binding mac_address port chassis/slot/port address ip_address vlan vlan_id
```

**Syntax Definitions**

- `mac_address` The client MAC address.
- `chassis` The chassis identifier.
- `slot1/port[1-port2]` The slot and port number (3/1).
- `ip_address` The IP address that the DHCP server offered to the client.
- `vlan_id` The VLAN identification number (1–4094).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900V72/C32</th>
<th>6900</th>
<th>6900X48C6/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Static binding table entries are created using this command. If DHCP Snooping binding table functionality is not enabled, creating a static entry is not allowed.
- Dynamic binding table entries are created when the relay agent receives a DHCPACK packet.
- Use the `no` form of this command to remove a static entry from the DHCP Snooping binding table.

**Examples**

```
-> dhcp-snooping binding 00:2a:95:51:6c:10 port 1/1/15 address 17.15.3.10 vlan 200
```

```
-> no dhcp-snooping binding 00:2a:95:51:6c:10 port 1/1/15 address 17.15.3.10 vlan 200
```

**Release History**

Release 7.3.4; command introduced.
Related Commands

**dhcp-snooping binding timeout**  Configures the amount of time between each automatic save of the binding table contents to a file on the switch.

**dhcp-snooping binding action**  Synchronizes the contents of the DHCP Snooping binding table with the contents of the `dhcpBinding.db` file saved on the switch.

**show dhcp-snooping binding**  Displays the contents of the DHCP Snooping binding table (database).

MIB Objects

dhcpSnoopingBindingTable
dhcpSnoopingBindingMacAddress
dhcpSnoopingBindingIfIndex
dhcpSnoopingBindingIpAddress
dhcpSnoopingBindingVlan
dhcpSnoopingBindingRowStatus
show dhcp-snooping

Displays the global DHCP Snooping configuration.

show dhcp-snooping

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When DHCP Snooping is enabled for the switch or for a specific VLAN, the DHCP Snooping binding database status is automatically enabled and additional fields are displayed.

- When DHCP Snooping is enabled at the switch level, the “Option 82 Data Insertion Per Switch” and “MAC Address Verification Per Switch” fields are displayed; these fields do not display when DHCP Snooping is enabled at the VLAN level.

Examples

-> show dhcp-snooping
DHCP Snooping :
  DHCP Snooping Status = Disabled
  DHCP Snooping Bypass Opt82-Check = Disabled,
  DHCP Snooping Opt82 Format = Base MAC,
  DHCP Snooping Opt82 String = 2c:fa:a2:13:e4:02,
  DHCP Snooping Binding DB Status = Disabled,
  DHCP Snooping Option-82 Policy = Replace,

-> dhcp-snooping admin-state enable
-> show dhcp-snooping
DHCP Snooping :
  DHCP Snooping Status = Switch-Level Enabled,
  Option 82 Data Insertion Per Switch = Enabled,
  MAC Address Verification Per Switch = Enabled,
  DHCP Snooping Bypass Opt82-Check = Disabled,
  DHCP Snooping Opt82 Format = Base MAC,
  DHCP Snooping Opt82 String = 2c:fa:a2:13:e4:02,
DHCP Snooping Binding DB Status = Enabled,
Database Sync Timeout = 1,
Database Last Sync Time = Oct 25 2016 14:56,
Binding Persistency Status = Disabled,
DHCP Snooping Option-82 Policy = Replace,

-> dhcp-snooping vlan 200 admin-state enable
-> show dhcp-snooping

DHCP Snooping:
DHCP Snooping Status = VLAN-Level,
DHCP Snooping Bypass Opt82-Check = Disabled,
DHCP Snooping Opt82 Format = Base MAC,
DHCP Snooping Opt82 String = 2c:fa:a2:13:e4:02,
DHCP Snooping Binding DB Status = Enabled,
Database Sync Timeout = 1,
Database Last Sync Time = Oct 28 2016 07:36,
Binding Persistency Status = Disabled,
DHCP Snooping Option-82 Policy = Replace,

output definitions

<table>
<thead>
<tr>
<th>DHCP Snooping Status</th>
<th>Displays whether DHCP Snooping is enabled at the Switch-Level, VLAN-Level, or Disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option 82 Data Insertion Per Switch</td>
<td>Indicates whether or not (Enabled or Disabled) the relay agent inserts the Option-82 field into DHCP packets before forwarding them to the DHCP server. Configured through the dhcp-snooping option-82-data-insertion command.</td>
</tr>
<tr>
<td>MAC Address Verification Per Switch</td>
<td>Indicates whether or not (Enabled or Disabled) the source MAC address is compared to the client hardware MAC address in the DHCP packet; if there is a mismatch the packet is dropped. Configured through the dhcp-snooping mac-address-verification command.</td>
</tr>
<tr>
<td>DHCP Snooping Bypass Opt82-Check</td>
<td>Indicates whether DHCP packets received on untrusted ports are checked to see if they contain the Option-82 field (Disabled) or not checked (Enabled). Configured through the dhcp-snooping bypass option-82-check command.</td>
</tr>
<tr>
<td>DHCP Snooping Opt82 Format</td>
<td>Displays the type of Option-82 information inserted into the Circuit ID and Remote ID suboptions of the Option-82 field. Configured through the dhcp-snooping option-82 format command.</td>
</tr>
<tr>
<td>DHCP Snooping Opt82 string</td>
<td>Displays the contents of the Option-82 string that is inserted into the Circuit ID and Remote ID suboptions of the Option-82 field.</td>
</tr>
<tr>
<td>DHCP Snooping Binding DB Status</td>
<td>Displays whether the DHCP Snooping binding table functionality is Enabled or Disabled. Configured through the dhcp-snooping binding admin-state command.</td>
</tr>
<tr>
<td>Database Sync Timeout</td>
<td>The amount of time, in seconds, between each automatic save of the DHCP Snooping binding table contents maintained in memory to a file on the switch. Configured through the dhcp-snooping binding timeout command.</td>
</tr>
<tr>
<td>Database Last Sync Time</td>
<td>The last date and time DHCP Snooping binding table entries were saved from memory to a file on the switch.</td>
</tr>
</tbody>
</table>
Output definitions

| Binding Persistency Status | Indicate whether a binding table entry is retained (Enabled) or removed (Disabled) if the MAC address is missing from the MAC address table when the binding table database is synchronized. Configured through the dhcp-snooping binding persistency command. |
| DHCP Snooping Option-82 Policy | Indicate whether to keep, replace, or drop the Option-82 field information contained in DHCP packets received by the switch. Configured through the dhcp-snooping option-82 policy command. |

Release History

Release 7.3.4; command introduced.

Related Commands

- dhcp-snooping admin-state Enables or disables DHCP Snooping for the switch.
- dhcp-snooping vlan Enables or disables DHCP Snooping at the VLAN level.

MIB Objects

- dhcpSnoopingMode
- dhcpSnoopingOpt82DataInsertionStatus
- dhcpSnoopingMacAddrVerificationStatus
- dhcpSnoopingBypassOpt82CheckStatus
- dhcpSnoopingOption82FormatType
- dhcpSnoopingOption82StringValue
- dhcpSnoopingOption82Policy
- dhcpSnoopingBindingStatus
- dhcpSnoopingBindingDatabaseSyncTimeout
- dhcpSnoopingBindingDatabaseLastSyncTime
- dhcpSnoopingBindingPersistencyStatus
show dhcp-snooping ip-source-filter

Displays the ports or VLANs on which IP source filtering is enabled.

show dhcp-snooping ip-source-filter {vlan | port}

**Syntax Definitions**

- **vlan** Displays the VLANs on which IP source filtering is enabled.
- **port** Displays the ports on which IP source filtering is enabled.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The show output displays only those ports or VLANs on which IP source filtering is enabled.
- This command also displays the status of the link aggregate ports when source filtering is enabled at VLAN or port level.

**Examples**

-> show dhcp-snooping ip-source-filter port

Global Admin Status : Enabled

<table>
<thead>
<tr>
<th>IP Src</th>
<th>Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------</td>
</tr>
<tr>
<td>1/1/7</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/1/12</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/4/30</td>
<td>Enabled</td>
</tr>
<tr>
<td>1/4/35</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
show dhcp-snooping ip-source-filter vlan

Global Admin Status : Enabled

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>IP Src Filtering</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Enabled</td>
</tr>
<tr>
<td>11</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command introduced.
Release 8.6.R1; “Global Admin Status” field added.

Related Commands

dhcp-snooping ip-source-filter admin-state
  Enables or disabled the DHCP Snooping IP source filtering functionality for the switch.

dhcp-snooping ip-source-filter
  Enables or disables IP source filtering for a specific port, link aggregate, or VLAN.

MIB Objects

dhcpSnoopingIpSourceFilterAdminState
dhcpSnoopingSourceFilterVlanTable
  dhcpSnoopingSourceFilterVlanNumber
dhcpSnoopingSourceFilterVlanFilteringStatus
dhcpSnoopingPortTable
  dhcpSnoopingPortIpSourceFiltering
show dhcp-snooping vlan

Displays a list of VLANs that have DHCP Snooping enabled and whether or not MAC address verification and Option-82 data insertion is enabled for each VLAN.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command only applies if DHCP Snooping is enabled at the VLAN level.
- Use the show dhcp-snooping command to determine the status of DHCP Snooping at the switch level.

Examples

```bash
-> show dhcp-snooping vlan
VLAN   Admin  Opt82  MAC Addr
ID     State  Insertion Verification
-------+---------+----------+---------------------
  50    Enabled Enabled  Enabled
  60    Enabled Enabled  Enabled
 100    Enabled Disabled  Enabled
 200    Enabled Enabled  Disabled
 300    Disabled Enabled  Enabled
 1500   Disabled Disabled  Disabled
```

output definitions

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>The VLAN identification number for the DHCP Snooping VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>The administrative status of DHCP Snooping for the VLAN (Enabled or Disabled).</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Addr Verification</td>
<td>Indicates whether or not MAC address verification is enabled for the VLAN (Enabled or Disabled).</td>
</tr>
<tr>
<td>Opt-82 Insertion</td>
<td>Indicates whether or not Option-82 data insertion is enabled for the VLAN (Enabled or Disabled).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command introduced.
Release 8.6R1; “Admin State” field added.

**Related Commands**

- **dhcp-snooping vlan**
  - Enables or disables DHCP Snooping, MAC address verification, and Option-82 data insertion for the specified VLAN.
- **show dhcp-snooping**
  - Displays the current DHCP Snooping configuration.
- **show dhcp-snooping port**
  - Displays the trust mode and DHCP violation statistics for all switch ports that are filtered by DHCP Snooping.

**MIB Objects**

dhcpSnoopingVlanTable
  - dhcpSnoopingVlanNumber
  - dhcpSnoopingVlanMacAddrVerificationStatus
  - dhcpSnoopingVlanOpt82DataInsertionStatus
  - dhcpSnoopingVlanStatus
  - dhcpSnoopingVlanAdminState
show dhcp-snooping port

Displays the trust mode and DHCP Snooping violation statistics for all switch ports and link aggregates that are filtered by DHCP Snooping.

show dhcp-snooping port [chassis/slot/port | linkagg_id]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If DHCP Snooping is operating at the switch level, then information for all switch ports and link aggregates is displayed.

- If DHCP Snooping is operating at the VLAN level, then information for only those ports and link aggregates that are associated with a DHCP Snooping VLAN is displayed.

- The violation statistics displayed only apply to ports and link aggregates that are in the client only trust mode. When the trust mode for a port is changed from client-only to trusted or blocked, the violation counters are set to zero (0).

- Use specific port numbers and link aggregate ID to filter and enhance display.

Examples

-> show dhcp-snooping port

<table>
<thead>
<tr>
<th>Port</th>
<th>Trust Mode</th>
<th>Opt82 Violation</th>
<th>MAC Violation</th>
<th>Server Violation</th>
<th>Relay Violation</th>
<th>Binding Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/4/1</td>
<td>Blocked</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/4/2</td>
<td>Client</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/4/3</td>
<td>Client</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/4/4</td>
<td>Trusted</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/4/5</td>
<td>Client</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0/10</td>
<td>Trusted</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Port</td>
<td>Trust Mode</td>
<td>Opt82 Violation</td>
<td>MAC Violation</td>
<td>Server Violation</td>
<td>Relay Violation</td>
<td>Binding Violation</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
<td>----------------</td>
<td>---------------</td>
<td>------------------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Trust</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- show dhcp-snooping port 20

<table>
<thead>
<tr>
<th>Port</th>
<th>Trust Mode</th>
<th>Opt82 Violation</th>
<th>MAC Violation</th>
<th>Server Violation</th>
<th>Relay Violation</th>
<th>Binding Violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/20</td>
<td>Client</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**output definitions**

- **Port**: The chassis, slot, and port number or a link aggregate ID number.
- **Trust Mode**: The DHCP Snooping trust mode for the port (Blocked, Client, or Trusted). Configured through the `dhcp-snooping port` command.
- **Opt82 Violation**: The number of DHCP packets dropped due to a DHCP Snooping Option-82 violation.
- **MAC Violation**: The number of DHCP packets dropped due to a mismatch between the packet source MAC address and the client hardware address contained within the packet.
- **Server Violation**: The number of DHCP server packets dropped because they originated from outside the network or firewall.
- **Relay Violation**: The number of DHCP packets dropped because the packet included a relay agent IP address that was not 0.0.0.0.
- **Binding Violation**: The number of DHCP packets dropped due to a mismatch between packets received and binding table information.

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

- `show dhcp-snooping`: Displays the current DHCP Snooping configuration.
- `show dhcp-snooping vlan`: Displays a list of DHCP Snooping VLANs.
- `dhcp-snooping clear violation-counters`: Clears the DHCP violation counters.

**MIB Objects**

- `dhcpSnoopingPortTable`
- `dhcpSnoopingPortIfIndex`
- `dhcpSnoopingPortTrustMode`
- `dhcpSnoopingPortOption82Violation`
- `dhcpSnoopingPortMacAddrViolation`
- `dhcpSnoopingPortDhcpServerViolation`
- `dhcpSnoopingPortRelayAgentViolation`
- `dhcpSnoopingPortBindingViolation`
dhcp-snooping clear violation-counters

Clears the DHCP violation counters.

dhcp-snooping clear violation-counters {port chassis/slot/port[-port2]} | slot chassis/slot | linkagg agg_id | all}

---

**Syntax Definitions**

- **chassis/slot/port [-port2]**: Clear DHCP snooping violation counters for the specified physical port or range of ports.
- **chassis/slot**: Clear DHCP snooping violation counters for all ports of the specified slot.
- **agg_id**: Clear DHCP snooping violation counter for the specified link aggregate.
- **all**: Clear DHCP snooping violation counters on all ports.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the **port**, **slot**, or **linkagg** parameter options to clear the DHCP violation counters for a specific port, all ports on a chassis/slot, or a specific link aggregate.

---

**Examples**

- `-> dhcp-snooping clear violation-counters port 1/2`
- `-> dhcp-snooping clear violation-counters port 1/2/3`
- `-> dhcp-snooping clear violation-counters port 1/2/4-9`
- `-> dhcp-snooping clear violation-counters linkagg 5`
- `-> dhcp-snooping clear violation-counters slot 3/2`
- `-> dhcp-snooping clear violation-counters all`

---

**Release History**

Release 8.5R2; command introduced.
Related Commands

show dhcp-snooping port Displays the trust mode and DHCP Snooping violation statistics for all switch ports that are filtered by DHCP Snooping.

MIB Objects

dhcpSnoopingClearViolationTable
dhcpSnoopingClearViolationIfIndex
dhcpSnoopingClearViolationAction
**show dhcp-snooping counters**

Displays the DHCP Snooping/Relay global counters.

**show dhcp-snooping counters [slot chassis_id/slot_id]**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

NI counters display the cumulative value from requested NIs.

**Examples**

`-> show dhcp-snooping counters`

DHCP Discover Packets: 226,
DHCP Offer Packets: 226,
DHCP Request Packets: 226,
DHCP ACK Packets: 226,
DHCP NACK Packets: 0,
DHCP Release Packets: 10,
DHCP Decline Packets: 0,
DHCP Inform Packets: 10,
DHCP Renew Packets: 0,
Total Packet received in CMM: 2,
Binding error (TCAM Unavailable): 0,
Unknown/Malformed Packets Dropped: 0,
Packets received in CMM: 224,
Packets transmitted from CMM: 909,
Total ISF Packet Drop: 0

`-> show dhcp-snooping counters slot 1/1`

Packet received in CMM from NI: 472,
Packet transmitted from CMM to NI: 453,
Packets received in NI from CMM: 453,
Packets transmitted from NI to CMM: 472,
Total ISF Packet Drop: 453,
DHCP Relay Commands

show dhcp-snooping counters

output definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Discover Packets</td>
<td>Displays the number of Discover packets.</td>
</tr>
<tr>
<td>DHCP Offer Packets</td>
<td>Displays the number of Offer packets.</td>
</tr>
<tr>
<td>DHCP Request Packets</td>
<td>Displays the number of Request packets.</td>
</tr>
<tr>
<td>DHCP ACK Packets</td>
<td>Displays the number Acknowledged packets.</td>
</tr>
<tr>
<td>DHCP NACK Packets</td>
<td>Displays the number of negative acknowledged packets.</td>
</tr>
<tr>
<td>DHCP Release Packets</td>
<td>Displays the number of Release packets.</td>
</tr>
<tr>
<td>DHCP Decline Packets</td>
<td>Displays the number of Decline packets.</td>
</tr>
<tr>
<td>DHCP Inform Packets</td>
<td>Displays the number of Inform packets.</td>
</tr>
<tr>
<td>DHCP Renew Packets</td>
<td>Displays the number of Renew packets.</td>
</tr>
<tr>
<td>Total Packet received in CMM</td>
<td>Displays the total number of packets received in CMM.</td>
</tr>
<tr>
<td>Binding error (TCAM Unavailable)</td>
<td>Displays the number of Binding error.</td>
</tr>
<tr>
<td>Unknown/Malformed Packets Dropped</td>
<td>Displays the number of Unknown or Malformed packets dropped.</td>
</tr>
<tr>
<td>Packets received in CMM</td>
<td>Displays the number of packets received in CMM.</td>
</tr>
<tr>
<td>Packets transmitted from CMM</td>
<td>Displays the number of packets transmitted from CMM.</td>
</tr>
<tr>
<td>Total ISF Packet Drop</td>
<td>Displays the number of total ISF packets dropped.</td>
</tr>
<tr>
<td>Packets received in CMM from NI</td>
<td>Displays the number of packets received in CMM which is transmitted from NI.</td>
</tr>
<tr>
<td>Packets transmitted from CMM to NI</td>
<td>Displays the number of packets transmitted from CMM which is received in NI.</td>
</tr>
<tr>
<td>Packets received in NI from CMM</td>
<td>Displays the number of packets received in NI which is transmitted from CMM.</td>
</tr>
<tr>
<td>Packets transmitted from NI to CMM</td>
<td>Displays the number of packets transmitted from NI which is received in CMM.</td>
</tr>
</tbody>
</table>

Release History

Release 8.5R2; command introduced.

Related Commands

dhcp-snooping clear counters  Clears the global counters for DHCP Snooping/Relay.

MIB Objects

N/A
### dhcp-snooping clear counters

Clears the global and per NI counters for DHCP Snooping/Relay.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When this command is used, the counter statistics displayed with the `show dhcp-snooping counters` command are reset to zero.

**Examples**

```bash
-> dhcp-snooping clear counters
```

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- `show dhcp-snooping counters` Displays the DHCP snooping/Relay global counters. NI counters display the cumulative value from requested NIs.

**MIB Objects**

N/A
**show dhcp-snooping isf-statistics**

Displays the IP source filter (ISF) drop counters.

**show dhcp-snooping isf-statistics [vlan vlan_id]**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>C32</th>
<th>C6</th>
<th>C8</th>
<th>E200</th>
<th>C32E</th>
<th>C24C2</th>
<th>X24C2</th>
<th>X48C4E</th>
<th>X48C8</th>
<th>X48C6/T48C6</th>
<th>X48C6</th>
<th>X48C6/V48C8</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/V48C8</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 C32E/T24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `vlan` parameter to display counters for a specific VLAN ID.

**Examples**

`-> show dhcp-snooping isf-statistics`
Mode: Vlan based ISF

<table>
<thead>
<tr>
<th>Chassis</th>
<th>Slot</th>
<th>Vlan</th>
<th>Packets Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>10</td>
<td>300</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>10</td>
<td>400</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>11</td>
<td>500</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>11</td>
<td>600</td>
</tr>
</tbody>
</table>

`-> show dhcp-snooping isf-statistics vlan 10`
Mode: Vlan based ISF

<table>
<thead>
<tr>
<th>Chassis</th>
<th>Slot</th>
<th>Vlan</th>
<th>Packets Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>10</td>
<td>300</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>10</td>
<td>400</td>
</tr>
</tbody>
</table>

`-> show dhcp-snooping isf-statistics`
Mode: Port based ISF

<table>
<thead>
<tr>
<th>Chassis</th>
<th>Slot</th>
<th>Vlan</th>
<th>Packets Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>NA</td>
<td>300</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>NA</td>
<td>400</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>NA</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>----</td>
<td>---</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

```
dhcp-snooping clear isf-statistics
```

Clears the ISF drop counters.

**MIB Objects**

N/A
**dhcp-snooping clear isf-statistics**

Clears the IP source filter (ISF) drop counters.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When this command is used, the counter statistics displayed with the `show dhcp-snooping isf-statistics` command are reset to zero.

**Examples**

```
-> dhcp-snooping clear isf-statistics
```

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- `show dhcp-snooping isf-statistics` Displays the ISF drop counters.

**MIB Objects**

N/A
show dhcp-snooping binding

Displays the contents of the DHCP Snooping binding table (database).

```
show dhcp-snooping binding [port chassis/slot/port] | linkagg agg_id | ip-address ip_address | snapshot [static | dynamic]]
```

### Syntax Definitions

- **chassis/slot/port**: The chassis, slot, and port number for which binding table entries are displayed.
- **agg_id**: The link aggregate ID for which binding table entries are displayed.
- **ip_address**: The IPv4 address for which binding table entries are displayed.
- **snapshot**: Displays binding table entries in the configuration snapshot format.
- **static**: Displays only static binding table entries.
- **dynamic**: Displays only dynamic binding table entries.

### Defaults

By default, all binding table entries are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `dhcp-snooping binding` command to create a static entry in the binding table.
- Dynamic binding table entries are created when the relay agent receives a DHCPACK packet.

### Examples

```
-> show dhcp-snooping binding

Total Number of Binding Entries: 12

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Port</th>
<th>IP Address</th>
<th>Lease Time</th>
<th>VLAN ID</th>
<th>Binding Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:20:95:11:22:10</td>
<td>1/1/4</td>
<td>100.100.100.10</td>
<td>-</td>
<td>100</td>
<td>Static</td>
</tr>
<tr>
<td>02:00:00:00:0a:00</td>
<td>1/1/5</td>
<td>100.100.100.11</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>00:20:95:11:22:11</td>
<td>1/1/5</td>
<td>100.100.100.20</td>
<td>-</td>
<td>100</td>
<td>Static</td>
</tr>
<tr>
<td>02:00:00:00:02:00</td>
<td>1/1/6</td>
<td>100.100.100.10</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>02:00:00:00:09:00</td>
<td>1/1/6</td>
<td>100.100.100.18</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>
```
show dhcp-snooping binding

Total Number of Binding Entries: 2

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Port</th>
<th>IP Address</th>
<th>Lease</th>
<th>VLAN</th>
<th>Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:00:00:00:08:00</td>
<td>1/6</td>
<td>100.100.100.6</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>02:00:00:00:05:00</td>
<td>1/6</td>
<td>100.100.100.8</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>02:00:00:00:03:00</td>
<td>1/7</td>
<td>100.100.100.3</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>02:00:00:00:01:00</td>
<td>1/7</td>
<td>100.100.100.17</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>02:00:00:00:07:00</td>
<td>0/1</td>
<td>100.100.100.13</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>02:00:00:00:04:00</td>
<td>0/1</td>
<td>100.100.100.15</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>00:20:95:11:22:12</td>
<td>0/10</td>
<td>100.100.100.30</td>
<td></td>
<td>100</td>
<td>Static</td>
</tr>
</tbody>
</table>

-> show dhcp-snooping binding port 1/1/5

Total Number of Binding Entries: 2

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Port</th>
<th>IP Address</th>
<th>Lease</th>
<th>VLAN</th>
<th>Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:00:00:00:0a:00</td>
<td>1/5</td>
<td>100.100.100.11</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>00:20:95:11:22:11</td>
<td>1/5</td>
<td>100.100.100.20</td>
<td></td>
<td>100</td>
<td>Static</td>
</tr>
</tbody>
</table>

-> show dhcp-snooping binding linkagg 1

Total Number of Binding Entries: 2

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Port</th>
<th>IP Address</th>
<th>Lease</th>
<th>VLAN</th>
<th>Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:00:00:00:07:00</td>
<td>0/1</td>
<td>100.100.100.13</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
<tr>
<td>02:00:00:00:04:00</td>
<td>0/1</td>
<td>100.100.100.15</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>

-> show dhcp-snooping binding ip-address 100.100.100.11

Total Number of Binding Entries: 1

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Port</th>
<th>IP Address</th>
<th>Lease</th>
<th>VLAN</th>
<th>Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:00:00:00:0a:00</td>
<td>1/5</td>
<td>100.100.100.11</td>
<td>30</td>
<td>100</td>
<td>Dynamic</td>
</tr>
</tbody>
</table>

-> show dhcp-snooping binding snapshot static
dhcp-snooping binding 00:20:95:11:22:12 linkagg 10 address 100.100.100.30 vlan 100
dhcp-snooping binding 00:20:95:11:22:10 port 1/1/4 address 100.100.100.10 vlan 100
dhcp-snooping binding 00:20:95:11:22:11 port 1/1/5 address 100.100.100.20 vlan 100

-> show dhcp-snooping binding snapshot dynamic
dhcp-snooping binding 02:00:00:00:0a:00 port 1/1/5 address 100.100.100.11 vlan 100
dhcp-snooping binding 02:00:00:00:02:00 port 1/1/6 address 100.100.100.10 vlan 100
dhcp-snooping binding 02:00:00:00:09:00 port 1/1/6 address 100.100.100.18 vlan 100
dhcp-snooping binding 02:00:00:00:08:00 port 1/1/6 address 100.100.100.6 vlan 100
dhcp-snooping binding 02:00:00:00:05:00 port 1/1/6 address 100.100.100.8 vlan 100
dhcp-snooping binding 02:00:00:00:03:00 port 1/1/7 address 100.100.100.3 vlan 100
dhcp-snooping binding 02:00:00:00:01:00 port 1/1/7 address 100.100.100.17 vlan 100
dhcp-snooping binding 02:00:00:00:07:00 linkagg 1 address 100.100.100.13 vlan 100
dhcp-snooping binding 02:00:00:00:04:00 linkagg 1 address 100.100.100.15 vlan 100

output definitions

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>The MAC address of the client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The chassis/slot/port designation for the switch port that received the DHCP request.</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 25-178
**Release History**

Release 7.3.4; command introduced.
Release 8.5R2; **snapshot, static, dynamic** parameters added.
Release 8.6R1; **port, linkagg, ip-address** parameters added.

**Related Commands**

- `show dhcp-snooping` Displays the current DHCP Snooping configuration.
- `show dhcp-snooping vlan` Displays a list of DHCP Snooping VLANs.
- `show dhcp-snooping port` Displays the trust mode and DHCP violation statistics for all switch ports that are filtered by DHCP Snooping.

**MIB Objects**

- `dhcpSnoopingBindingStatus`
- `dhcpSnoopingBindingTable`
  - `dhcpSnoopingBindingMacAddress`
  - `dhcpSnoopingBindingIfIndex`
  - `dhcpSnoopingBindingIpAddress`
  - `dhcpSnoopingBindingLeaseTime`
  - `dhcpSnoopingBindingVlan`
  - `dhcpSnoopingBindingType`

---

**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address offered by the DHCP server.</td>
</tr>
<tr>
<td>Lease Time</td>
<td>The IP address lease time assigned by the DHCP server. A value of 0 indicates a static entry.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>The VLAN ID of the VLAN to which the client belongs.</td>
</tr>
<tr>
<td>Binding Type</td>
<td>Indicates whether the binding table entry is <strong>dynamic</strong> or <strong>static</strong>. Static entries are created using the <code>dhcp-snooping binding</code> command.</td>
</tr>
</tbody>
</table>
**dhcpv6-snooping vlan admin-state**

Enables or disables DHCPv6 Snooping on a per-VLAN basis.

```
dhcpv6-snooping vlan vlan_id[-vlan_id2] admin-state {enable | disable}

no dhcpv6-snooping vlan vlan_id[-vlan_id2]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`: The VLAN ID on which DHCPv6 Snooping must be enabled or disabled. Use a hyphen to specify a range of VLANs (10-15).
- `enable`: Enables DHCPv6 Snooping on the specified VLAN.
- `disable`: Disables DHCPv6 Snooping on the specified VLAN.

**Defaults**

By default, this feature is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- DHCPv6 Snooping can be enabled on per-VLAN basis or globally on the switch.
- The global DHCPv6 Snooping must be disabled before enabling the per-VLAN DHCPv6 Snooping.
- When DHCPv6 Snooping is configured on a per-VLAN basis, DHCPv6 snooping is limited to a maximum of 64 VLANs.
- DHCPv6 snooping must not be enabled in configurations where a DHCPv6 server assigns multiple addresses to a client. In such situations, only the first address will be stored in the binding table.
- To completely remove DHCPv6 snooping configuration from a VLAN, use the `no` form of the command.

**Examples**

```
-> dhcpv6-snooping vlan 1 admin-state enable
-> dhcpv6-snooping vlan 10-20 admin-state enable
-> dhcpv6-snooping vlan 1 admin-state disable
-> dhcpv6-snooping vlan 10-20 admin-state disable
-> no dhcpv6-snooping vlan 2
-> no dhcpv6-snooping vlan 10-20
```
**Release History**

Release 8.5R3; command introduced.
Release 8.6R2; VLAN range added.

**Related Commands**

- `dchpv6-snooping binding` Configures a static entry in the binding table.
- `dchpv6-snooping binding persistency` Configures whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.
- `dchpv6-snooping ipv6-source-filter` Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level using the DHCPv6 Snooping binding table.
- `show dchpv6-snooping` Displays the global DHCPv6 Snooping configuration.
- `show dchpv6-snooping interfaces` Displays the DHCPv6 Snooping configuration status on per-VLAN.

**MIB Objects**

- `alaiDHCPv6SnoopingTable`
  - `alaiDHCPv6SnoopingInterfaceIndex`
  - `alaiDHCPv6SnoopingInterfaceAdminStatus`
  - `alaiDHCPv6SnoopingInterfaceRowStatus`
**dhcpv6-snooping global admin-state**

Enables or disables DHCPv6 Snooping globally on the switch.

```
dhcpv6-snooping global admin-state {enable | disable}
```

### Syntax Definitions

- **global**
  - The DHCPv6 Snooping is enabled or disabled globally on the switch.

- **enable**
  - Enables DHCPv6 Snooping for the switch.

- **disable**
  - Disables DHCPv6 Snooping for the switch.

### Defaults

By default, this feature is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- DHCPv6 Snooping can be enabled on per-VLAN or globally on the switch.
- The per-VLAN DHCPv6 Snooping must be disabled before enabling global DHCPv6 Snooping.
- DHCPv6 snooping must not be enabled in configurations where a DHCPv6 server assigns multiple addresses to a client. In such situations only the first address will be stored in the binding table.

### Examples

- `-> dhcpv6-snooping global admin-state enable`
- `-> dhcpv6-snooping global admin-state disable`

### Release History

Release 8.5R3; command introduced.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dhcpv6-snooping binding</code></td>
<td>Configures a static entry in the binding table.</td>
</tr>
<tr>
<td><code>dhcpv6-snooping binding persistency</code></td>
<td>Allows to configure whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.</td>
</tr>
<tr>
<td><code>dhcpv6-snooping ipv6-source-filter</code></td>
<td>Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level using the DHCPv6 Snooping binding table.</td>
</tr>
<tr>
<td><code>show dhcpv6-snooping</code></td>
<td>Displays the global DHCPv6 Snooping configuration.</td>
</tr>
<tr>
<td><code>show dhcpv6-snooping interfaces</code></td>
<td>Displays the DHCPv6 Snooping configuration status on per-VLAN.</td>
</tr>
</tbody>
</table>

**MIB Objects**

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>alaDHCPv6SnoopingTable</code></td>
<td></td>
</tr>
<tr>
<td><code>alaDHCPv6SnoopingInterfaceIndex</code></td>
<td></td>
</tr>
<tr>
<td><code>alaDHCPv6SnoopingInterfaceAdminStatus</code></td>
<td></td>
</tr>
<tr>
<td><code>alaDHCPv6SnoopingInterfaceRowStatus</code></td>
<td></td>
</tr>
</tbody>
</table>
**dhcpv6-snooping binding**

Configures a static entry in the binding table.

```
dhcpv6-snooping binding vlan vlan_id link-local ipv6_address [global-address ipv6_address] [mac-address mac_address] [port chassis/slot/port | linkagg agg_id]
```

```
no dhcpv6-snooping binding vlan vlan_id link-local ipv6_address
```

---

**Syntax Definitions**

- `vlan_id` The VLAN ID on which the DHCPv6 client is configured.
- `link-local` The clients link-local IPv6 address.
- `global-address` The IPv6 global unicast address assigned by the DHCPv6 lease server.
- `mac-address` The clients MAC address.
- `port | linkagg` The port or link aggregate used to reach the DHCPv6 client.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When a new binding entry is added or an existing entry is modified using this command, the entry's lease lifetime is changed to indefinite.
- While adding a new binding entry the values for all the parameters must be specified. Else, the binding entry will not be added.
- When a VLAN is deleted, all binding entries on the VLAN including the manually added binding entry is also removed.

**Examples**

```
-> dhcpv6-snooping binding vlan 1 link-local fe80:eaee7:32ff:fe4a:6321 global-address 2001:db8:1000::2b0:d0ff:fe86:880e mac-address 00:00:01:1d:4f:7d linkagg 1
```

```
-> no dhcpv6-snooping binding vlan 1 link-local fe80:eaee7:32ff:fe4a:6321
```

**Release History**

Release 8.5R3; command introduced.
Related Commands

**dhcpv6-snooping global admin-state**  Enables or disables DHCPv6 Snooping globally on the switch.

**dhcpv6-snooping vlan admin-state**  Enables or disables DHCPv6 Snooping on a per-VLAN basis.

**show dhcpv6-snooping binding**  Displays the DHCPv6 Snooping binding table information.

MIB Objects

<table>
<thead>
<tr>
<th>Object Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaDHCPv6BindingTable</td>
</tr>
<tr>
<td>alaDHCPv6SnoopingInterfaceIndex</td>
</tr>
<tr>
<td>alaDHCPv6BindingLinkLocalAddress</td>
</tr>
<tr>
<td>alaDHCPv6BindingGlobalAddress</td>
</tr>
<tr>
<td>alaDHCPv6BindingPhysAddress</td>
</tr>
<tr>
<td>alaDHCPv6BindingPortIfIndex</td>
</tr>
</tbody>
</table>
**dhcpv6-snooping binding timeout**

Configures the amount of time between each automatic save of the DHCPv6 Snooping binding table contents maintained in memory to a file on the switch.

**dhcpv6-snooping binding timeout seconds**

---

**Syntax Definitions**

```
seconds
```

The time interval in seconds between automatic save of the DHCPv6 Snooping binding table to file on the switch. The time interval range is 1 to 600 seconds.

**Defaults**

The default value is 1 second.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The timeout value is only valid if the DHCPv6 Snooping binding table functionality is enabled.

---

**Examples**

```
-> dhcpv6-snooping binding timeout 5
```

---

**Release History**

Release 8.5R3; command introduced.

---

**Related Commands**

- **dhcpv6-snooping binding** Configures a static entry in the binding table.
- **show dhcpv6-snooping binding** Displays the DHCPv6 Snooping binding table information.

---

**MIB Objects**

- **alaDHCPV6BindingConfig**
- **alaDHCPv6BindingTimeout**
**dhcpv6-snooping binding action**

Allows to manually purge, renew or save the DHCPv6 Snooping binding table.

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>purge</td>
<td>Clears the content of the DHCPv6 binding table.</td>
</tr>
<tr>
<td>renew</td>
<td>Restores the DHCPv6 binding table entries with the previously saved values in the permanent storage.</td>
</tr>
<tr>
<td>save</td>
<td>Saves the DHCPv6 binding table entries to permanent storage.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C8/C32E/T24C2/</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The DHCPv6 Snooping binding table is maintained in the switch memory. Binding table entries are saved on a periodic basis to the file on the switch. Use the purge, renew, and save options available with this command to sync the binding table contents with the contents of the file.

- While using binding table action commands ensure the binding timeout interval is set greater than 10 seconds from the default interval 1 second to avoid quick timeout.

**Examples**

- `-> dhcpv6-snooping binding action purge`
- `-> dhcpv6-snooping binding action renew`
- `-> dhcpv6-snooping binding action save`

**Release History**

Release 8.5R3; command introduced.
Related Commands

**dhcpv6-snooping binding**  Configures a static entry in the binding table.

**show dhcpv6-snooping binding**  Displays the DHCPv6 Snooping binding table information.

MIB Objects

alaDHCPV6BindingConfig
alaDHCPv6BindingAction
**dhcpv6-snooping binding persistency**

Configures whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.

**Syntax Definitions**

| enable | Enables DHCPv6 Snooping binding persistency. The DHCPv6 Snooping binding table entries will be retained even if the MAC address is deleted from the switch's MAC cache. |
| disable | Disables DHCPv6 Snooping binding persistency. The DHCPv6 Snooping binding table entries will be deleted if the MAC address is deleted from the switch's MAC cache. |

**Defaults**

By default, DHCPv6 snooping binding persistency is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the binding table is restored from permanent storage when the DHCPv6 Snooping binding persistency is enabled, all entries will be added to the binding table, even if the MAC address is not in the switch's MAC cache.

- If the binding table is restored from permanent storage when the DHCPv6 Snooping binding persistency is disabled, only entries for which there is a corresponding entry in the switch's MAC cache will be restored.

- The binding entries will get deleted upon lease time expiry and also during link down or MAC address deletion unless persistency is enabled on the switch.

**Examples**

- `-> dhcpv6-snooping binding persistency enable`
- `-> dhcpv6-snooping binding persistency disable`

**Release History**

Release 8.5R3; command introduced.
**Related Commands**

*show dhcpv6-snooping binding*  Displays the DHCPv6 Snooping binding table information.

**MIB Objects**

alaDHCPV6BindingConfig

alaDHCPv6BindingPersistency
**dhcppv6-snooping ipv6-source-filter**

Enables or disables the IPv6 source filtering capability for a port, link aggregate, or VLAN using the DHCPv6 Snooping binding table.

```
dhcppv6-snooping ipv6-source-filter {vlan vlan_id[-vlan_id2] | port chassis/slot1/port[-port2] | linkagg agg_id[-agg_id2]} admin-state {enable | disable}
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` The VLAN ID on which the IPv6 source filtering needs to be enabled or disabled. Use a hyphen to specify a range of VLAN IDs (10-15).
- `chassis/slot1/port[-port2]` The port number on which the IPv6 source filtering needs to be enabled or disabled. Use a hyphen to specify a range of ports (1/1/3-8).
- `agg_id[-agg_id2]` The linkagg ID on which the IPv6 source filtering needs to be enabled or disabled. Use a hyphen to specify a range of IDs (1-5).
- `enable` Enables IPv6 source filtering for the specified port, link aggregation, or VLAN.
- `disable` Disables IPv6 source filtering for the specified port, link aggregation, or VLAN level.

**Defaults**

By default, IPv6 source filtering is disabled on port, link aggregation, or VLAN level.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- DHCPv6 Snooping must be enabled for IPv6 source filtering to be enabled.
- IPv6 source filtering can be enabled per-VLAN or per-port (linkagg).
- If DHCPv6 Snooping is enabled on switch level, then IPv6 source filtering can be enabled on any port, linkagg or VLAN.
- If DHCPv6 Snooping is enabled on VLAN, then IPv6 source filtering can only be enabled on ports which are part of that VLAN, or on the same VLAN.
- If a static host is connected to IPv6 source filtering enabled port or VLAN, then all the packets coming from this host are dropped. A static binding entry must be created to allow the packets coming from this host to pass.
To support IPv6 source filtering on an OmniSwitch 6560 and OmniSwitch 6570M, use the `capability profile tcam mode` command to set the TCAM mode to source IPv6 filtering. After the TCAM mode is changed, reboot the switch to activate the source IPv6 filtering mode.

**Examples**

- `-> dhcpv6-snooping ipv6-source-filter vlan 1 admin-state enable`
- `-> dhcpv6-snooping ipv6-source-filter vlan 10-15 admin-state enable`
- `-> dhcpv6-snooping ipv6-source-filter port 1/1/2 admin-state enable`
- `-> dhcpv6-snooping ipv6-source-filter port 1/1/3-8 admin-state enable`
- `-> dhcpv6-snooping ipv6-source-filter linkagg 6 admin-state enable`
- `-> dhcpv6-snooping ipv6-source-filter linkagg 1-5 admin-state enable`
- `-> dhcpv6-snooping ipv6-source-filter vlan 1 admin-state disable`
- `-> dhcpv6-snooping ipv6-source-filter vlan 10-15 admin-state disable`
- `-> dhcpv6-snooping ipv6-source-filter port 1/1/2 admin-state disable`
- `-> dhcpv6-snooping ipv6-source-filter port 1/1/3-8 admin-state disable`
- `-> dhcpv6-snooping ipv6-source-filter linkagg 6 admin-state disable`
- `-> dhcpv6-snooping ipv6-source-filter linkagg 1-5 admin-state disable`

**Release History**

Release 8.5R3; command introduced.
Release 8.6R2; VLAN, port, and link aggregate range added.

**Related Commands**

- `dhcpv6-snooping vlan admin-state` Enables or disables DHCPv6 Snooping on a per-VLAN basis.
- `dhcpv6-snooping global admin-state` Enables or disables DHCPv6 Snooping globally on the switch.
- `show dhcpv6-snooping ipv6-source-filter` Displays the port, VLAN or link aggregation on which IPv6 Source Filter (ISF) is configured.

**MIB Objects**

- `alaDHCPV6SourceFilterInterfaceTable`
  - `alaDHCPV6SourceFilterVlanId`
  - `alaDHCPV6SourceFilterInterfaceIfIndex`
  - `alaDHCPV6SourceFilterInterfaceRowStatus`
  - `alaDHCPV6SourceFilterVlanRowStatus`
**ipv6 dhcp guard**

Enables or disables DHCPv6 Guard on a VLAN or a VLAN range. If enabled (the default), DHCPv6 server messages are discarded unless the messages are received on trusted ports. This command also includes an option to enable DHCPv6 Guard for client messages.

```
ipv6 dhcp guard vlan vlan_id [-vlan_id] [client {enable | disable}] [admin-state {enable | disable}]
no ipv6 dhcp guard vlan vlan_id [-vlan_id]
```

**Syntax Definitions**

- `vlan_id[-vlan_id]` A VLAN ID number or a range of VLAN IDs on which the DHCPv6 Guard is configured. The valid range is 1–4094. Use a hyphen to specify a range of VLAN IDs (21-30).
- `client enable` Enables DHCPv6 Guard for client messages. Multicast client-originated messages are sent out only on trusted ports. If there are no configured trusted ports, the client messages are dropped.
- `client disable` Disables DHCPv6 Guard for client messages. Client-originated messages are not checked.
- `admin-state enable` Enables DHCPv6 guard for server messages. DHCPv6 server messages that are not received on configured trusted ports are dropped. Enabling DHCPv6 Guard helps to prevent access from rogue DHCPv6 servers.
- `admin-state disable` Disables DHCPv6 Guard. Server messages are not checked.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>client enable</td>
<td>disable</td>
</tr>
<tr>
<td>admin-state enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Trusted source ports serve as a filtering mechanism and are identified using the `ipv6 dhcp guard trusted` command.
  - Only DHCPv6 server messages received on trusted ports are allowed.
  - Client multicast messages are sent out only on trusted ports rather than flooded out on all ports in the VLAN.
- Enabling DHCPv6 Guard without configuring any trusted ports helps to prevent unwanted DHCPv6 traffic flow. For example:
  - DHCPv6 server messages are discarded, which helps to prevent messages from reaching clients on the VLAN.
  - If the client option is also enabled, then DHCPv6 multicast client messages are also discarded. This helps to prevent DHCPv6 traffic from getting past the switch. If there are no client messages sent out, then there are no responses sent from the DHCPv6 server.
- Use the `no` form of this command to remove the DHCPv6 Guard configuration, which includes removing any configured trusted ports for the VLAN.

**Examples**

```plaintext
-> ipv6 dhcp guard vlan 200 admin-state enable
-> ipv6 dhcp guard vlan 200 admin-state disable
-> ipv6 dhcp guard vlan 200 client enable
-> ipv6 dhcp guard vlan 200 client disable
-> no ipv6 dhcp guard vlan 200
```

**Release History**

Release 8.5R2; command introduced.
Release 8.6R1; `vlan` and `client` parameters added, `if_name` parameter deprecated.
Release 8.8R1; support for VLAN range added.

**Related Commands**

- `ipv6 dhcp guard trusted` Configures the DHCPv6 Guard trusted source ports.
- `show ipv6 dhcp guard` Displays the DHCPv6 Guard configuration.

**MIB Objects**

alaDHCPv6GuardInterfaceTable
  alaDHCPv6GuardInterfaceEntry
  alaDHCPv6GuardInterfaceAdminStatus
  alaDHCPv6GuardInterfaceClient
  alaDHCPv6GuardInterfaceRowStatus
**ipv6 dhcp guard trusted**

Configures the DHCPv6 Guard trusted source ports.

```
ipv6 dhcp guard vlan vlan_id trusted [port chassis/slot/port [-port2]] | linkagg agg_id[-agg_id2]]
no ipv6 dhcp guard vlan vlan_id trusted [port chassis/slot/port [-port2]] | linkagg agg_id[-agg_id2]]
```

**Syntax Definitions**

- `vlan_id` The VLAN ID on which DHCPv6 Guard is configured.
- `chassis/slot/port [-port2]` The chassis/slot/port on which the DHCPv6 server messages must be allowed. Use a hyphen to specify a range of ports (3/1-10). Make sure the port is a member of the specified VLAN.
- `agg_id[-agg_id2]` The link aggregate ID on which the DHCPv6 server messages must be allowed. Use a hyphen to specify a range of IDs (10-15). Make sure the link aggregate ID is a member of the specified VLAN.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When DHCPv6 Guard is enabled, trusted source ports serve as a filtering mechanism.
  - Only DHCPv6 server messages received on trusted ports are allowed. This functionality helps to prevent access from rogue DHCPv6 servers.
  - Client multicast messages are sent out only on trusted ports rather than flooded out on all ports in the VLAN.
- Enabling DHCPv6 Guard without configuring any trusted ports helps to prevent unwanted DHCPv6 traffic flow. For example:
  - DHCPv6 server messages are discarded, which helps to prevent messages from reaching clients on the VLAN.
  - DHCPv6 multicast client messages are also discarded, which helps to prevent DHCPv6 traffic from getting past the switch. If there are no client messages sent out, then there are no responses sent from the DHCPv6 server.
- Use the **no** form of the command to remove the DHCPv6 Guard trusted source.
Examples

-> ipv6 dhcp guard vlan 200 trusted port 2/1/11
-> ipv6 dhcp guard vlan 200 trusted linkagg 10
-> no ipv6 dhcp guard vlan 200 trusted port 2/1/11

Release History

Release 8.5R2; command introduced.
Release 8.6R1; vlan parameter added, if_name parameter deprecated.
Release 8.8R1; support for port range and link aggregate range added.

Related Commands

ipv6 dhcp guard
   Enables or disables the DHCPv6 Guard on a VLAN.
show ipv6 dhcp guard
   Displays the DHCPv6 Guard configuration.

MIB Objects

alaDHCPv6GuardTrustedSourceTable
   alaDHCPv6GuardTrustedSourceIfIndex
   alaDHCPv6GuardTrustedSourceRowStatus
show dhcpv6-snooping

Displays the global DHCPv6 Snooping configuration.

show dhcpv6-snooping

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show dhcpv6-snooping
DHCPv6 Snooping = Global,
Binding timeout (sec) = 1,
Binding persistency = Disabled

output definitions

<table>
<thead>
<tr>
<th>Output Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Snooping</td>
<td>Displays if the DHCPv6 Snooping is enabled globally or Per-VLAN mode.</td>
</tr>
<tr>
<td>Binding timeout</td>
<td>Displays the binding table automatic save timeout.</td>
</tr>
<tr>
<td>Binding persistency</td>
<td>Displays the configured DHCPv6 Relay destination(s) for the interface.</td>
</tr>
</tbody>
</table>

Release History

Release 8.5R3; command introduced.
Related Commands

**dhcpv6-snooping vlan admin-state**
Enables or disables DHCPv6 Snooping on a per-VLAN basis.

**dhcpv6-snooping global admin-state**
Enables or disables DHCPv6 Snooping globally on the switch.

**dhcpv6-snooping binding timeout**
Configures the amount of time between each automatic save of the DHCPv6 Snooping binding table contents maintained in memory to a file on the switch.

**dhcpv6-snooping binding persistency**
Configures whether to retain or not retain the entries in the DHCPv6 Snooping binding table for the duration of the lease, regardless of the existence of the MAC address in the MAC address table.

MIB Objects

alaDHCPv6SnoopingInterfaceAdminStatus
alaDHCPv6BindingTimeout
alaDHCPv6BindingPersistency
show dhcpv6-snooping interfaces

Displays the DHCPv6 Snooping configuration status per-VLAN.

show dhcpv6-snooping interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show dhcpv6-snooping interfaces

Interface   Admin Status
VLAN 11     Enabled
VLAN 99     Disabled

output definitions

| Interface | Displays the VLAN on which DHCPv6 Snooping is configured. |
| Admin Status | Displays the operational status of DHCPv6 Snooping on the VLAN interface. |

Release History

Release 8.5R3; command introduced.
**Related Commands**

- `dhcpv6-snooping vlan admin-state` Enables or disables DHCPv6 Snooping on a per-VLAN basis.
- `dhcpv6-snooping global admin-state` Enables or disables DHCPv6 Snooping globally on the switch.

**MIB Objects**

- `alaDHCPv6SnoopingInterfaceIndex`
- `alaDHCPv6SnoopingInterfaceAdminStatus`
**show dhcpv6-snooping binding**

Displays the DHCPv6 Snooping binding table information.

```
show dhcpv6-snooping binding [global-address ipv6_address] [port chassis/slot/port | linkagg agg_id]
```

### Syntax Definitions

- **ipv6_address**
  - The IPV6 global unicast address for which binding table entries are displayed.

- **chassis/slot/port**
  - The chassis, slot, and port number for which binding table entries are displayed.

- **agg_id**
  - The link aggregate ID for which binding table entries are displayed.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show dhcpv6-snooping binding
Total Number of Binding Entries: 3
  Link-Local Address  Global Address  Lifetime  Interface  Port   MAC Address
  +-------------------+---------------+----------+----------+------+-----------------
  fe80::02aa:81ff:febb:0101  2001:db8:11::1  2000       VLAN 11    1/1/1  00:AA:81:BB:01:01
  fe80::02aa:81ff:febb:0202  2001:db8:11::2  indefinite VLAN 11    1/1/2  00:AA:81:BB:02:02

-> show dhcpv6-snooping binding port 1/1/1
Total Number of Binding Entries: 1
  fe80::02aa:81ff:febb:0101  2001:db8:11::1  2000       VLAN 11    1/1/1  00:AA:81:BB:01:01

-> show dhcpv6-snooping binding global-address 2001:db8:11::2
Total Number of Binding Entries: 1
  fe80::02aa:81ff:febb:0202  2001:db8:11::2  indefinite VLAN 11    1/1/2  00:AA:81:BB:02:02
```
show dhcpv6-snooping binding

Total Number of Binding Entries: 1

Link-Local Address  Global Address  Lifetime  Interface  Port  MAC Address
-----------------------------------------------------------------------------

Release History

Release 8.5R3; command introduced.

Related Commands

dhcpv6-snooping binding
  Configures a static entry in the binding table.

dhcpv6-snooping binding timeout
  Allows to configure the amount of time between each automatic save of the DHCPv6 Snooping binding table contents maintained in memory to a file on the switch.

dhcpv6-snooping binding action
  Allows to manually purge, renew or save the DHCPv6 Snooping binding table.

MIB Objects

alaDHCPv6BindingLinkLocalAddress
alaDHCPv6BindingPortIfIndex
alaDHCPv6BindingLeasedAddress
alaDHCPv6BindingLeaseTime
alaDHCPv6BindingType
alaDHCPv6SnoopingInterfaceIndex
alaDHCPv6BindingPhysAddress

output definitions

<table>
<thead>
<tr>
<th>Total Number of Binding Entries</th>
<th>The total number of binding entries in the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link-Local Address</td>
<td>The link-local address of the client.</td>
</tr>
<tr>
<td>Global Address</td>
<td>The global IPv6 address obtained through the DHCPv6 lease.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The lifetime of the DHCPv6 lease. The lifetime is displayed in seconds. The lifetime is displayed as indefinite for the leases with indefinite lifetime. The lifetime is displayed as static if the time is manually configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>The VLAN on which the client exists.</td>
</tr>
<tr>
<td>Port</td>
<td>The physical port or link aggregation used to communicate with the client.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the client.</td>
</tr>
</tbody>
</table>
show dhcpv6-snooping ipv6-source-filter

Displays the port, VLAN or link aggregation on which IPv6 Source Filter (ISF) is configured.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show dhcpv6-snooping ipv6-source-filter

Mode: Vlan based ISF

VLAN ID
--------
10-15
20

-> show dhcpv6-snooping ipv6-source-filter

Mode: Port based ISF

PORT
-----
1/1/10
1/1/15-20
0/2
DHCP Relay Commands  

**show dhcpv6-snooping ipv6-source-filter**

**output definitions**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Displays the VLAN on which the ISF is enabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>PORT</td>
<td>Displays the port or link aggregation on which the ISF is enabled.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R3; command introduced.

**Related Commands**

`dhcpv6-snooping ipv6-source-filter` Enables or disables the IPv6 source filtering capability at a port, link aggregation, or VLAN level using the DHCPv6 Snooping binding table.

**MIB Objects**

- `alaDHCPv6SourceFilterVlanId`
- `alaDHCPv6SourceFilterInterfaceIfIndex`
show ipv6 dhcp guard

Displays the DHCPv6 Guard configuration.

```
show ipv6 dhcp guard [vlan vlan_id]
```

### Syntax Definitions

- **vlan_id**
  
  Displays the DHCPv6 Guard configuration for the specified VLAN.

### Defaults

By default, a summary table of information about all VLANs on which DHCPv6 Guard is configured is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Specify the `vlan vlan_id` option to view the DHCPv6 Guard configuration for a specific VLAN.

### Examples

```
-> show ipv6 dhcp guard
Interface                        Status   Client   Trusted Ports
--------------------------------+--------+--------+--------------------------------
VLAN 200                         Enabled  Disabled 1/1/9, 1/1/10, 1/1/11, 1/1/12+
VLAN 250                         Enabled  Disabled
VLAN 300                         Enabled  Enabled  agg 10, 1/4/20
```

#### output definitions

- **Interface**
  
  Displays the VLAN on which the DHCPv6 Guard is configured.

- **Status**
  
  Displays the status of DHCPv6 Guard (**Enabled** or **Disabled**).

- **Client**
  
  Displays the status of DHCPv6 Guard for client messages (**Enabled** or **Disabled**).

- **Trusted Ports**
  
  Displays the DHCPv6 Guard trusted sources. A '+' will appear at the end of the list to indicate that there are more trusted sources configured which cannot be displayed in a single line. To view the full list of configured trusted sources, specify the VLAN ID in the show command.
-> show ipv6 dhcp guard vlan 200
DHCPv6 Guard = Enabled
Client Guard = Disabled
Trusted ports:
   1/1/9
   1/1/10
   1/1/11
   1/1/12
   1/1/20

-> show ipv6 dhcp guard vlan 250
DHCPv6 Guard = Enabled
Client Guard = Disabled

-> show ipv6 dhcp guard vlan 300
DHCPv6 Guard = Enabled
Client Guard = Enabled
Trusted ports:
   linkagg 10
   1/4/20

output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCPv6 Guard</td>
<td>Displays the status of DHCPv6 Guard on the VLAN.</td>
</tr>
<tr>
<td>Client Guard</td>
<td>Displays the status of DHCPv6 Guard for client messages.</td>
</tr>
<tr>
<td>Trusted ports</td>
<td>Displays the DHCPv6 Guard trusted sources, if any. Ports are displayed as</td>
</tr>
<tr>
<td></td>
<td>chassis/slot/port. Link aggregates are displayed as linkagg ID.</td>
</tr>
</tbody>
</table>

Release History

Release 8.5R2; command introduced.
Release 8.561; vlan parameter added.

Related Commands

ipv6 dhcp guard  Enables or disables the DHCPv6 Guard on a VLAN.
ipv6 dhcp guard trusted Configures DHCPv6 Guard trusted source ports.

MIB Objects

alaDHCPv6GuardInterfaceTable
   AlaDHCPv6GuardInterfaceEntry
   alaDHCPv6GuardInterfaceAdminStatus
   alaDHCPv6GuardInterfaceClient
alaDHCPv6GuardTrustedSourceTable
   alaDHCPv6GuardTrustedSourceIfIndex
The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure in a default route environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the IPv4 or IPv6 VRRP routers on the LAN. The VRRP router that controls the IPv4 or IPv6 address associated with a virtual router is called the master router and is responsible for forwarding packets to that IPv4 or IPv6 address. If the master router becomes unavailable, the highest priority backup router will transition to the master state. The OmniSwitch implementation of VRRP also supports the collective management of virtual routers on a switch.

The VRRP commands comply with RFC 3768 for VRRP version 2 (IPv4) and RFC 5798 for VRRP version 3 (IPv4 and IPv6).

MIB information is as follows:

- **Filename**: VRRP-MIB.mib
  **Module**: vrrpMIB

- **Filename**: VRRPv3-MIB.mib
  **Module**: vrrp3MIB

- **Filename**: ALCATEL-IND1-VRRP-MIB.mib
  **Module**: alcatelIND1VRRPMIB

- **Filename**: ALCATEL-IND1-VRRPv3-MIB.mib
  **Module**: alcatelIND1VRRP3MIB
A summary of the available VRRP commands is listed here:

---

vrrp
vrrp address
vrrp track
vrrp bfd-state
vrrp track-association
vrrp delay
vrrp version
vrrp interval
vrrp priority
vrrp preempt
vrrp accept
vrrp admin-state
vrrp set
vrrp group
vrrp group admin-state
vrrp group set
vrrp group-association
show vrrp
show vrrp statistics
show vrrp track
show vrrp track-association
show vrrp group
show vrrp group-association
---
vrrp

Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.

```
{ip | ipv6} vrrp vrid interface if_name admin-state [enable | disable] [priority priority] [preempt | no preempt] [accept | no accept] [interval centiseconds] [version {v2 | v3}]
```

```
no {ip | ipv6} vrid interface if_name
```

### Syntax Definitions

- **ip**
  - Configures an IPv4 virtual router.

- **ipv6**
  - Configures an IPv6 virtual router.

- **vrid**
  - The virtual router ID. The valid range is 1–255.

- **if_name**
  - The name of an existing IPv4 or IPv6 interface on which the virtual router is configured.

- **enable**
  - Enables the virtual router. An IPv4 virtual router may only be enabled if an IP address is configured for the virtual router (not required to enable an IPv6 virtual router).

- **disable**
  - Disables the virtual router. Cannot be combined on the same line with other parameters.

- **priority**
  - The priority for this virtual router to become the master router. The range is 1 (lowest priority) to 255 (highest priority). The priority should be set to 255 only if this router is the actual owner of the virtual router’s IP address.

- **preempt**
  - Specifies that a higher priority router may preempt a lower priority master router. However, the virtual router's actual IP address owner will always preempt another master router regardless of whether preempt is enabled.

- **no preempt**
  - Specifies that a higher priority router may not preempt a lower priority master router.

- **accept**
  - Specifies that the master router, which is not the IP address owner, will accept the packets addressed to the IP address owner as its own. *This parameter applies only to IPv4 version 3 and IPv6 virtual routers.*

- **no accept**
  - Specifies that the master router, which is not the IP address owner, will not accept the packets addressed to the IP address owner as its own. *This parameter applies only to IPv4 version 3 and IPv6 virtual routers.*

- **centiseconds**
  - The interval in centiseconds after which the master router will send VRRP advertisements. The advertising interval must be the same for all VRRP routers configured with the same VRID. The valid interval ranges are as follows:
    - 1–25500 centiseconds for VRRP version 2 router.
    - 1–4095 centiseconds for VRRP version 3 router.

- **v2**
  - Converts an IPv4 VRRP router to a version 2 virtual router. *This parameter applies only to IPv4 virtual routers; IPv6 virtual routers are always version 3.*
v3

Converts an IPv4 VRRP router to a version 3 virtual router. *This parameter applies only to IPv4 virtual routers; IPv6 virtual routers are always version 3.*

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>priority</td>
<td>100</td>
</tr>
<tr>
<td>preempt</td>
<td>no preempt</td>
</tr>
<tr>
<td>accept</td>
<td>no accept</td>
</tr>
<tr>
<td>centiseconds</td>
<td>100</td>
</tr>
<tr>
<td>v2</td>
<td>v3</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a virtual router from the configuration.
- Use the `ip vrrp address` command to configure an IPv4 address for the virtual router. This must be done before the IPv4 virtual router can be enabled (not required to enable an IPv6 virtual router).
- To disable the virtual router, rather than remove it, use the `admin-state disable` option. Note that this option cannot be used with any other optional parameter.
- Do not disable a virtual router when it is the address owner without first disabling the IP interface. Failure to do so may result in duplicate IP address errors.
- A virtual router must be disabled before it can be modified.
- A priority value of 255 indicates that the VRRP router owns the IP address; that is, the router contains the real physical interface to which the IP address is assigned. The system automatically sets this value to 255 if it detects that this router is the IP address owner. If the priority is set to 255 and the virtual router is not the IP address owner, then the priority will be set to the default value of 100. The IP address owner will always be the master router if it is available.
- VRRP routers backing up a virtual router must use priority values from 1 to 255. The default priority value for VRRP routers backing up a virtual router is 100. If you configure more than one backup, their priority values should be different. The `preempt` or `no preempt` setting specifies whether or not a higher priority router may preempt a lower priority master router.
• The maximum number of virtual routers supported is based on the 100 centisecond advertising interval. A smaller interval will result in a relatively lesser number of virtual routers.

• The VRRP router version (v2 or v3) determines the advertising interval value range and the level of granularity that is used to specify the interval value. For example:
  – The advertising interval range for VRRP version 2 is 1–25500 and cannot be less than 100 centiseconds. The interval value should also be entered in increments of 100 (for example, 100, 200, 300) up to the maximum allowed. If the interval value is not specified in an increment of 100, then the value is rounded down to the next increment of 100. For example, if a value of 209 is specified, then that value is rounded down to 200.
  – The advertising interval range for VRRP version 3 is 1–4095 and cannot be less than 10 centiseconds. The interval value should also be entered in increments of 10 (for example, 10, 20, 30) up to the maximum allowed. If the interval value is not specified in an increment of 10, then the value is rounded down to the next increment of 10. For example, if a value of 15 is specified, then that value is rounded down to 10.

Examples

-> ip vrrp 23 interface ipv4-100 priority 75
-> ip vrrp 23 interface ipv4-100 address 192.168.173.1
-> ip vrrp 23 interface ipv4-100 admin-state enable

-> ip vrrp 23 interface ipv4-100 admin-state disable
-> ip vrrp 23 interface ipv4-100 priority 255
-> ip vrrp 23 interface ipv4-100 admin-state enable
-> no ip vrrp 23 interface ipv4-100

-> ip vrrp 28 interface v4if-v150 interval 30000
ERROR: Advertisement interval must be between 1 and 25500

-> ipv6 vrrp 33 interface ipv6-200 priority 75
-> ipv6 vrrp 33 interface ipv6-200 admin-state enable

-> ipv6 vrrp 33 interface ipv6-200 admin-state disable
-> ipv6 vrrp 33 interface ipv6-200 priority 50
-> ipv6 vrrp 33 interface ipv6-200 admin-state enable
-> no ipv6 vrrp 33 interface ipv6-200

-> ipv6 vrrp 44 interface "v6if-v200" interval 4096
ERROR: Advertisement interval must be between 1 and 4095 for version V3

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; interface and version parameter added; vlan_id parameter deprecated.
Release 8.7R2; VRRP router advertising interval range updated.
Related Commands

- **vrrp address**
  Configures an IPv4 or an IPv6 address for a virtual router.

- **show vrrp**
  Displays the virtual router configuration for all virtual routers or for a specific virtual router.

### MIB Objects

- **vrrpv3OperationsTable**
  - **vrrpv3OperationsPriority**
  - **vrrpv3OperationsPreemptMode**
  - **vrrpv3OperationsAcceptMode**
  - **vrrpv3OperationsAdvInterval**
  - **vrrpv3OperationsRowStatus**

- **alaVrrpv3OperationsExTable**
  - **alaVrrpv3OperVersion**
vrrp address

Configures an IPv4 or IPv6 address for a VRRP virtual router.

{ip | ipv6} vrrp vrid interface if_name address {ipv4_address | ipv6_address}
{ip | ipv6} vrrp vrid interface if_name no address {ipv4_address | ipv6_address}

Syntax Definitions

ip                  Configures an IPv4 address for a virtual router.
ipv6                Configures an IPv6 address for a virtual router.
vrid                The virtual router ID. The valid range is 1–255.
if_name             The name of an existing IPv4 or IPv6 interface on which the virtual
                    router is configured.
ipv4_address        The virtual IPv4 address to associate with the specified virtual router.
ipv6_address        The virtual IPv6 address to associate with the specified virtual router.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

An IPv4 address must be configured for an IPv4 virtual router before the virtual router can be enabled (not required to enable an IPv6 virtual router).

Examples

-> ip vrrp 23 interface ipv4-100 address 192.168.173.1
-> ip vrrp 23 interface ipv4-100 address 192.168.173.2
-> ip vrrp 23 interface ipv4-100 no address 192.168.173.1

-> ipv6 vrrp 33 interface ipv6-200 213:100:1::56
-> ipv6 vrrp 33 interface ipv6-200 213:100:1::57
-> ipv6 vrrp 33 interface ipv6-200 no address 213:100:1::56
**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; **interface** parameter added; **vlan_id** and optional **ip** parameter deprecated.

**Related Commands**

- **vrrp**
  Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.

- **show vrrp**
  Displays the virtual router configuration for all virtual routers or for a specific virtual router.

- **show vrrp statistics**
  Displays statistics about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

**MIB Objects**

- **vrrpv3AssociatedIpAddrTable**

  **vrrpv3AssociatedIpAddrRowStatus**
vrrp track

Creates a new tracking policy or modifies an existing tracking policy.

```
ip vrrp track track_id [admin-state [enable | disable] | priority priority | ipv4-interface if_name | ipv6-interface if_name | port chassis/slot/port | address ip_address [bfd-state {enable | disable} | delay seconds]]
```

```
no ip vrrp track track_id
```

Syntax Definitions

- **track_id**: The ID of the tracking policy. The valid range is 1–255.
- **admin-state enable**: Enables the tracking policy.
- **admin-state disable**: Disables the tracking policy.
- **priority**: The decrement priority value. A virtual router monitoring this tracking policy will have its priority decremented by this value when the conditional state of the tracking policy entity is down. The valid range is 0–255.
- **if_name**: The name of the IPv4 or IPv6 interface that this policy will track.
- **chassis**: The chassis identifier.
- **slot/port**: The slot/port number that this policy will track.
- **ip_address**: The remote IPv4 or IPv6 address that this policy will track.
- **bfd-state enable**: Enables Bidirectional Forwarding Detection (BFD) for an address tracking policy. This parameter is not supported on the OmniSwitch 6560 and OmniSwitch 6570M.
- **bfd-state disable**: Disables BFD for an address tracking policy. This parameter is not supported on the OmniSwitch 6560 and OmniSwitch 6570M.
- **delay seconds**: The amount of time to wait after a VRRP address track is detected as operationally up and before the associated virtual router's priority value is incremented by the tracking policy's priority value. The valid range is 0–60 seconds.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-state enable</td>
<td>disable</td>
</tr>
<tr>
<td>priority</td>
<td>25</td>
</tr>
<tr>
<td>bfd-state enable</td>
<td>disable</td>
</tr>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to remove a tracking policy.
- Use the **admin-state disable** option to disable the tracking policy, rather than removing it from the switch.
- Registering VRRP with BFD is required at the protocol level before VRRP can interact with BFD. Once VRRP is a registered protocol with BFD, then BFD can be enabled for a specific VRRP address tracking policy.
- Enabling BFD for an address tracking policy requires a Loopback0 interface on the local switch. The IP address of this interface will serve as the source IP address of BFD packets. For more information about configuring a Loopback0 interface, see the “IP Commands” or “IPv6 Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.
- Configuring the delay time for an IPv4 address or IPv6 address tracking policy helps to prevent the loss of device connectivity that may occur before a virtual router prematurely becomes the master. For example, configuring a delay time allows the switch routing tables to stabilize before the master router resumes the master role.

Examples

```
-> ip vrrp track 2 admin-state enable priority 50 ipv4-interface Marketing
-> ip vrrp track 3 admin-state enable priority 60 ipv6-interface Sales
-> ip vrrp track 2 address 10.1.1.1 bfd-state enable
-> ip vrrp track 3 address 10.1.1.2 delay 30
-> ip vrrp track 4 address 10.1.1.2 bfd-state enable delay 45
-> ip vrrp track 5 address 20.1.1.12 bfd-state enable delay 45
-> ip vrrp track 2 address 10.1.1.12 bfd-state enable delay 45
-> no ip vrrp track 2
```

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **delay** parameter added.
**Related Commands**

**vrrp track-association**
Associates a VRRP tracking policy with a virtual router.

**vrrp bfd-state**
Enables or disables the BFD protocol for VRRP.

**show vrrp track**
Displays information about tracking policies on the switch.

**MIB Objects**

alaVRRPTrackTable
- alaVrrpTrackId
- alaVrrpTrackState
- alaVrrpTrackAdminState
- alaVrrpTrackPriority
- alaVrrpTrackEntityType
- alaVrrpTrackEntityPort
- alaVrrpTrackEntityIpAddrType
- alaVrrpTrackEntityIpAddress
- alaVrrpTrackEntityIpv6Interface
- alaVrrpTrackEntityInterface
- alaVrrpTrackBfdStatus
- alaVrrpTrackDelay
- alaVrrpTrackRowStatus
vrrp bfd-state

Enables or disables the registration of VRRP with the BFD protocol.

```
ip vrrp bfd-state {enable | disable}
```

**Syntax Definitions**

- **enable**: Enables BFD for VRRP.
- **disable**: Disables BFD for VRRP.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- BFD interaction with VRRP is supported only for VRRP tracking policies that track a remote IP address.
- BFD must be globally enabled for the switch and VRRP must be registered with BFD at the protocol level before VRRP can interact with BFD.

**Examples**

```
-> ip bfd admin-state enable
-> ip vrrp bfd-state enable
-> ip vrrp bfd-state disable
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **vrrp track**
  - Configures an address tracking policy.

- **ip bfd admin-state**
  - Enables or disables the global BFD protocol status for the switch.

- **show vrrp**
  - Displays the virtual router configuration for all virtual routers or for a specific virtual router

MIB Objects

- **alaVrrpConfig**
  - **alaVrrpBfdStatus**
vrrp track-association

Associates an IPv4 or IPv6 VRRP tracking policy with a virtual router.

\{ip | ipv6\} vrrp vrid interface if_name track-association track_id
\{ip | ipv6\} vrrp vrid interface if_name no track-association track_id

Syntax Definitions

ip Associates a tracking policy with an IPv4 virtual router.
ipv6 Associates a tracking policy with an IPv6 virtual router.
vrid The virtual router ID. The valid range is 1–255.
if_name The name of an existing IPv4 or IPv6 interface on which the virtual router is configured.
track_id The ID of the tracking policy to associate with the virtual router. The valid range is 1–255.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove a tracking policy from a virtual router.
- The tracking policy ID must already exist in the switch configuration. Use the vrrp track command to create a tracking policy.

Examples

- \(\rightarrow\) ip vrrp 23 interface ipv4-100 track-association 1
- \(\rightarrow\) ip vrrp 23 interface ipv4-100 no track-association 1

- \(\rightarrow\) ipv6 vrrp 33 interface ipv6-200 track-association 1
- \(\rightarrow\) ipv6 vrrp 33 interface ipv6-200 no track-association 1
**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; `interface` parameter added; `vlan_id` parameter deprecated.

**Related Commands**

- **vrrp**
  - Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.

- **vrrp track**
  - Configures a VRRP or VRRP3 tracking policy.

- **show vrrp track-association**
  - Displays the tracking policies associated with virtual routers.

**MIB Objects**

alaVrrp3AssoTrackTable
- alaVrrp3AssoTrackId
- alaVrrp3TrackRowStatus
**vrrp delay**

Configures the amount of time allowed for routing tables to stabilize before virtual routers are started.

```
   ip vrrp delay seconds
```

**Syntax Definitions**

- `seconds` The amount of time after a reboot that virtual routers will wait before they go active. The valid range is 0–180 seconds.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>45 seconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to prevent loss of workstation connectivity before a virtual router becomes master.

**Examples**

```
   -> ip vrrp delay 50
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

**vrrp**
Configures a new VRRP virtual router or modifies an existing one. Used to enable or disable a virtual router.

**show vrrp**
Displays the virtual router configuration for all virtual routers or for a specific virtual router.

**MIB Objects**

`alaVRRPConfig`

`alaVRRPStartDelay`
vrrp version

Modifies the default VRRP version assigned to the IPv4 virtual routers on the switch. The VRRP version for IPv6 virtual routers is not configurable (IPv6 virtual routers support only version 3).

ip vrrp version [v2 | v3]

Syntax Definitions

| v2 | Assigns version 2 by default to IPv4 virtual routers. |
| v3 | Assigns version 3 by default to IPv4 virtual routers. |

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>v2</td>
<td>v2</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Modifying the default VRRP version will affect the version assigned by default to any new IPv4 virtual routers that are created.

- To apply the new default value to the existing IPv4 virtual routers, first disable the virtual routers, then apply the new default value using the `ip vrrp set version` command and enable the virtual routers again.

- If any of the IPv4 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the `ip vrrp set version` command with the `override` option and enable the virtual routers again.

- There is no interoperability between VRRP version 2 and 3. A version 3 virtual router will not acknowledge version 2 advertisements.

- The VRRP router version (`v2` or `v3`) determines the advertising interval value range and the level of granularity that is used to specify the interval value. For example:
  - The advertising interval range for VRRP version 2 is 1–25500 and cannot be less than 100 centiseconds. The interval value should also be entered in increments of 100 (for example, 100, 200, 300) up to the maximum allowed.
  - The advertising interval range for VRRP version 3 is 1–4095 and cannot be less than 10
centiseconds. The interval value should also be entered in increments of 10 (for example, 10, 20, 30) up to the maximum allowed.

**Examples**

```
-> ip vrrp version v3
-> ip vrrp version v2

-> ip vrrp admin-state disable
-> ip vrrp set version
-> ip vrrp set version override
-> ip vrrp admin-state enable
```

**Release History**

Release 8.5R2; command introduced.

**Related Commands**

- **vrrp admin-state**: Changes the administrative status of all the virtual routers on the switch.
- **vrrp set**: Sets the new default parameter values to existing virtual routers on the switch.
- **show vrrp**: Displays the virtual router configuration for all virtual routers or for a specific virtual router.

**MIB Objects**

- `alaVRRPv3IPv4Config`
- `alaVRRPv3IPv4DefaultVersion`
**vrrp interval**

Modifies the default advertising interval value assigned to the IPv4 or IPv6 virtual routers on the switch.

```
{ip | ipv6} vrrp interval centiseconds
```

### Syntax Definitions

- **ip**: Modifies the default advertising interval value assigned to IPv4 virtual routers.
- **ipv6**: Modifies the default advertising interval value assigned to IPv6 virtual routers.
- **centiseconds**: The default advertising interval to assign to IPv4 (version 2 or 3) virtual routers or IPv6 (version 3) virtual routers.
  - 1–25500 centiseconds for a VRRP version 2 router.
  - 1–4095 centiseconds for a VRRP version 3 router.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>centiseconds</td>
<td>100</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Modifying the default advertising interval value will affect the value assigned by default to any new IPv4 or IPv6 virtual routers that are created.

- To apply the new default value to existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the **ip vrrp set interval** or **ipv6 vrrp set interval** command and enable the virtual routers again.

- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the **ip vrrp set interval** or **ipv6 vrrp set interval** command with the **override** option and enable the virtual routers again.
The VRRP router version (v2 or v3) determines the advertising interval value range and the level of granularity that is used to specify the interval value. For example:

- The advertising interval range for VRRP version 2 is 1–25500 and cannot be less than 100 centiseconds. The interval value should also be entered in increments of 100 (for example, 100, 200, 300) up to the maximum allowed. If an interval value is not specified in an increment of 100, then the value is rounded down to the next increment of 100. For example, if a value of 209 is specified, then that value is rounded down to 200.

- The advertising interval range for VRRP version 3 is 1–4095 and cannot be less than 10 centiseconds. The interval value should also be entered in increments of 10 (for example, 10, 20, 30) up to the maximum allowed. If the interval value is not specified in an increment of 10, then the value is rounded down to the next increment of 10. For example, if a value of 15 is specified, then that value is rounded down to 10.

Examples

```
-> ip vrrp interval 30000
ERROR: Advertisement interval must be between 1 and 25500
-> ip vrrp interval 200
-> ip vrrp admin-state disable
-> ip vrrp set interval
-> ip vrrp set interval override
-> ip vrrp admin-state enable

-> ipv6 vrrp interval 4096
ERROR: Advertisement interval must be between 1 and 4095 for version V3
-> ipv6 vrrp interval 75
-> ipv6 vrrp admin-state disable
-> ipv6 vrrp set interval
-> ipv6 vrrp set interval override
-> ipv6 vrrp admin-state enable
```

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.
Release 8.7R2; VRRP router advertising interval range updated.

Related Commands

```
**vrrp admin-state**
Changes the administrative status of all the virtual routers on the switch.

**vrrp set**
Sets the new default parameter values to existing virtual routers on the switch.

**show vrrp**
Displays the virtual router configuration for all virtual routers or for a specific virtual router.
```

MIB Objects

```
alaVRRPv3IPv4Config
alaVRRPv3IPv4DefaultInterval
alaVRRPv3IPv6Config
alaVRRPv3IPv6DefaultInterval
```
vrrp priority

Modifies the default priority value assigned to the IPv4 or IPv6 virtual routers on the switch.

{ip | ipv6} vrrp priority priority

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Modifies the default priority value assigned to IPv4 virtual routers.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Modifies the default priority value assigned to IPv6 virtual routers.</td>
</tr>
<tr>
<td>priority</td>
<td>The default priority value for the IPv4 or IPv6 virtual routers. The valid range is 1–255.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>100</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Modifying the default priority value will affect the value assigned by default to any new IPv4 or IPv6 virtual routers that are created.

- To apply the new default value to the existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the `ip vrrp set priority` or `ipv6 vrrp set priority` command and enable the virtual routers again.

- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the `ip vrrp set priority` or `ipv6 vrrp set priority` command with the `override` option and enable the virtual routers again.

Examples

- `-> ip vrrp priority 50`
- `-> ip vrrp admin-state disable`
- `-> ip vrrp set priority`
- `-> ip vrrp set priority override`
- `-> ip vrrp admin-state enable`
VRRP Commands

- ipv6 vrrp priority 75
- ipv6 vrrp admin-state disable
- ipv6 vrrp set priority
- ipv6 vrrp set priority override
- ipv6 vrrp admin-state enable

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

Related Commands

vrrp admin-state
Changes the administrative status of all the virtual routers on the switch.

vrrp set
Sets the new default parameter values to existing virtual routers on the switch.

show vrrp
Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

alaVRRPv3IPv4Config
  alaVRRPv3IPv4DefaultPriority
alaVRRPv3IPv6Config
  alaVRRPv3IPv6DefaultPriority
**vrrp preempt**

Modifies the default preempt mode assigned to the IPv4 or IPv6 virtual routers on the switch.

```
{ip | ipv6} vrrp [preempt | no preempt]
```

**Syntax Definitions**

- **ip**
  - Modifies the default preempt mode assigned to IPv4 virtual routers.
- **ipv6**
  - Modifies the default preempt mode assigned to IPv6 virtual routers.
- **preempt**
  - Specifies that a higher priority router may preempt a lower priority master router by default.
- **no preempt**
  - Specifies that a higher priority router may not preempt a lower priority master router by default.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>preempt</td>
<td>no preempt</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Modifying the default preempt mode will affect the mode assigned by default to any new IPv4 or IPv6 virtual routers that are created.

- To apply the new default value to the existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the `ip vrrp set preempt` or `ipv6 vrrp set preempt` command and enable the virtual routers again.

- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the `ip vrrp set preempt` or `ipv6 vrrp set preempt` command with the `override` option and enable the virtual routers again.

**Examples**

- `-> ip vrrp preempt`
- `-> ip vrrp no preempt`
- `-> ip vrrp admin-state disable`
VRRP Commands

VRRP Commands

- `ip vrrp set preempt`
- `ip vrrp set preempt override`
- `ip vrrp admin-state enable`
- `ipv6 vrrp preempt`
- `ipv6 vrrp no preempt`
- `ipv6 vrrp admin-state disable`
- `ipv6 vrrp set preempt`
- `ipv6 vrrp set preempt override`
- `ipv6 vrrp admin-state enable`

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

**Related Commands**

- `vrrp admin-state` Changes the administrative status of all the virtual routers on the switch.
- `vrrp set` Sets the new default parameter values to existing virtual routers on the switch.
- `show vrrp` Displays the virtual router configuration for all virtual routers or for a specific virtual router.

**MIB Objects**

- `alaVRRPv3IPv4Config`
  - `alaVRRPv3IPv4DefaultPreemptMode`
- `alaVRRPv3IPv6Config`
  - `alaVRRPv3IPv6DefaultPreemptMode`
vrrp accept

Modifies the default accept mode assigned to the IPv4 (version 3) or IPv6 virtual routers on the switch.

{ip | ipv6} vrrp [accept | no accept]

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Modifies the default accept mode assigned to IPv4 virtual routers.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Modifies the default accept mode assigned to IPv6 virtual routers.</td>
</tr>
<tr>
<td>accept</td>
<td>Specifies that the master router, which is not the IP address owner, will accept the packets addressed to the IP address owner as its own.</td>
</tr>
<tr>
<td>no accept</td>
<td>Specifies that the master router, which is not the IP address owner, will not accept the packets addressed to the IP address owner as its own.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>accept</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Modifying the default accept mode will affect the mode assigned by default to any new IPv4 or IPv6 virtual routers that are created.

- To apply the new default accept mode value to the existing IPv4 or IPv6 virtual routers, first disable the virtual routers, then apply the new default value using the ip vrrp set accept or ipv6 vrrp set accept command and enable the virtual routers again.

- If any of the IPv4 or IPv6 virtual routers are running with their own configured value or group value, then that value will take priority over the new default value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the ip vrrp set accept or ipv6 vrrp set accept command with the override option and enable the virtual routers again.

- The accept mode is not a configurable option for IPv4 virtual routers running VRRP version 2; this command only applies to IPv4 virtual routers running VRRP version 3 and IPv6 virtual routers.
Examples

- `ip vrrp accept`
- `ip vrrp no accept`
- `ip vrrp admin-state disable`
- `ip vrrp set accept`
- `ip vrrp set accept override`
- `ip vrrp admin-state enable`
- `ipv6 vrrp accept`
- `ipv6 vrrp no accept`

- `ipv6 vrrp admin-state disable`
- `ipv6 vrrp set accept`
- `ipv6 vrrp set accept override`
- `ipv6 vrrp admin-state enable`

Release History

Release 8.5R2; command was introduced.

Related Commands

vrrp admin-state
Changes the administrative status of all the virtual routers on the switch.

vrrp set
Sets the new default parameter values to existing virtual routers on the switch.

show vrrp
Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

alaVRRPv3IPv4Config
alaVRRPv3IPv4DefaultAcceptMode
alaVRRPv3IPv6Config
alaVRRPv3IPv6DefaultAcceptMode
**vrrp admin-state**

Changes the administrative status of all the IPv4 or IPv6 virtual routers on the switch.

```
{ip | ipv6} vrrp admin-state [disable | enable | enable-all]
```

**Syntax Definitions**

- **ip**: Changes the administrative status of all IPv4 virtual routers.
- **ipv6**: Changes the administrative status of all IPv6 virtual routers.
- **disable**: Disables all the IPv4 or IPv6 virtual routers on the switch.
- **enable**: Enables the IPv4 or IPv6 virtual routers that have not previously been disabled individually or collectively through the `ip vrrp group all` or `ipv6 vrrp group all` command.
- **enable-all**: Enables all the IPv4 or IPv6 virtual routers on the switch including those virtual routers that have been disabled individually or collectively through the `ip vrrp group all` or `ipv6 vrrp group all` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command changes the administrative status of all the IPv4 or IPv6 virtual routers on the switch by executing a single command.

- This command will not affect the ability to change the administrative status of an individual IPv4 or IPv6 virtual router.

**Examples**

```
-> ip vrrp admin-state disable
-> ip vrrp admin-state enable
-> ip vrrp admin-state enable-all

-> ipv6 vrrp admin-state disable
-> ipv6 vrrp admin-state enable
-> ipv6 vrrp admin-state enable-all
```
**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

**Related Commands**

- **vrrp version**
  Modifies the default VRRP version assigned to the IPv4 virtual routers on the switch.

- **vrrp interval**
  Modifies the default advertising interval value assigned to the virtual routers on the switch.

- **vrrp priority**
  Modifies the default priority value assigned to the virtual routers on the switch.

- **vrrp preempt**
  Modifies the default preempt mode assigned to the virtual routers on the switch.

- **vrrp accept**
  Modifies the default accept mode assigned to the virtual routers on the switch.

- **vrrp set**
  Sets the new default parameter values to existing virtual routers on the switch.

- **show vrrp**
  Displays the virtual router configuration for all virtual routers or for a specific virtual router.

**MIB Objects**

- alaVRRPv3IPv4Config
- alaVRRPv3IPv4AdminState
- alaVRRPv3IPv6Config
- alaVRRPv3IPv6AdminState
**vrrp set**

Applies the global default parameter values to IPv4 or IPv6 virtual routers on the switch. When this command is used, IPv4 or IPv6 virtual routers revert to using the default parameter values.

```
{ip | ipv6} vrrp set {interval | priority | preempt | accept | version | all | none} [override]
```

### Syntax Definitions

- **ip**: Applies the default parameter values to IPv4 virtual routers.
- **ipv6**: Applies the default parameter values to IPv6 virtual routers.
- **interval**: Sets the VRRP advertisement interval value to the default value.
- **priority**: Sets the priority value to the default value.
- **preempt**: Sets the preempt mode to the default mode.
- **accept**: Sets the accept mode to the default mode.
- **version**: Sets the VRRP version for IPv4 virtual routers to the default value.
- **all**: Sets all the parameters value to the new default value.
- **none**: Resets all the parameter values to their default values.
- **override**: Overrides the specified parameters configured value with the new default value.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval</td>
<td>all</td>
</tr>
<tr>
<td>priority</td>
<td>all</td>
</tr>
<tr>
<td>preempt</td>
<td>all</td>
</tr>
<tr>
<td>accept</td>
<td>all</td>
</tr>
<tr>
<td>version</td>
<td>all</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- All the IPv4 or IPv6 virtual routers must be disabled before using this command.
- When a new IPv4 or IPv6 virtual router is created, pre-defined default values for the advertising interval, priority, preempt mode, accept mode, and version (IPv4 only) parameters are applied to the new virtual router. These default parameter values are configurable. For example, the `ip vrrp interval` or `ipv6 vrrp interval` command is used to change the default interval value that is applied to IPv4 or IPv6 virtual routers.
• When a default parameter value is changed, however, it is not automatically applied to existing virtual routers. To apply default values that have changed to existing virtual routers, do the following:

1. Administratively disable all the virtual routers.
2. Use the `ip vrrp set` or `ipv6 vrrp set` command to apply the changed parameter value.
3. Administratively enable all the virtual routers.

• If any of the IPv4 or IPv6 virtual routers are running with their own individually configured value or group value, then that value takes priority over the default parameter value. To override the configured value with the new default value, first disable the virtual routers, then override the configured value using the `ip vrrp set` or `ipv6 vrrp set` command with the `override` option and enable the virtual routers again.

**Examples**

```
-> ip vrrp admin-state disable
-> ip vrrp set priority
-> ip vrrp set priority override
-> ip vrrp admin-state enable
-> ipv6 vrrp admin-state disable
-> ipv6 vrrp set interval
-> ipv6 vrrp set interval override
-> ipv6 vrrp admin-state enable
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; `accept` and `version` parameters added.

**Related Commands**

- `vrrp version` Modifies the default VRRP version assigned to the IPv4 virtual routers on the switch.
- `vrrp interval` Modifies the default advertising interval value assigned to the virtual routers on the switch.
- `vrrp priority` Modifies the default priority value assigned to the virtual routers on the switch.
- `vrrp preempt` Modifies the default preempt mode assigned to the virtual routers on the switch.
- `vrrp accept` Modifies the default accept mode assigned to the virtual routers on the switch.
- `vrrp admin-state` Changes the administrative status of all the virtual routers on the switch.
- `show vrrp` Displays the virtual router configuration for all virtual routers or for a specific virtual router.
MIB Objects

alaVRRPv3IPv4Config
  alaVRRPv3IPv4SetParam
  alaVRRPv3IPv4Override
alaVRRPv3IPv6Config
  alaVRRPv3IPv6SetParam
  alaVRRPv3IPv6Override
vrrp group

Creates a new IPv4 or IPv6 virtual router group or modifies the configuration parameters of an existing IPv4 or IPv6 virtual router group.

```
{ip | ipv6} vrrp group vrgid [interval centiseconds] [priority priority] [preempt | no preempt] [accept | no accept] [version {v2 | v3}]
```

no {ip | ipv6} vrrp group vrgid

### Syntax Definitions

- **ip**: Configures an IPv4 virtual router group.
- **ipv6**: Configures an IPv6 virtual router group.
- **vrgid**: The virtual router group ID. The valid range is 1–255.
- **centiseconds**: The interval in centiseconds after which the master router will send VRRP advertisements.
  - 1–25500 centiseconds for a VRRP version 2 router.
  - 1–4095 centiseconds for a VRRP version 3 router.
- **priority**: The default priority value for the virtual router group. The valid range is 1–255.
- **preempt**: Specifies that a higher priority router may preempt a lower priority master router.
- **no preempt**: Specifies that a higher priority router may not preempt a lower priority master router by default.
- **accept**: Specifies that the master router, which is not the IP address owner, will accept the packets addressed to the IP address owner as its own. This parameter applies only to IPv4 version 3 and IPv6 virtual routers.
- **no accept**: Specifies that the master router, which is not the IP address owner, will not accept the packets addressed to the IP address owner as its own. This parameter applies only to IPv4 version 3 and IPv6 virtual routers.
- **v2**: Converts an IPv4 VRRP router as a version 2 virtual router. This parameter applies only to IPv4 virtual routers.
- **v3**: Converts an IPv4 VRRP router to a version 3 virtual router. This parameter applies only to IPv4 virtual routers.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>centiseconds</td>
<td>100</td>
</tr>
<tr>
<td>priority</td>
<td>100</td>
</tr>
<tr>
<td>preempt</td>
<td>no preempt</td>
</tr>
<tr>
<td>accept</td>
<td>no accept</td>
</tr>
<tr>
<td>v2</td>
<td>v3</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to delete the virtual router group.
- The configuration parameters can be modified at any time, but will not have any effect on the virtual routers in the group until the virtual routers are enabled again. To apply the group default values to the virtual routers in a group, you must first disable the virtual router group, then apply the group default value using the ip vrrp group set or ipv6 vrrp group set command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their individually configured value, then that value will take priority over the new default value. To override the configured value with the new default value, you must first disable the virtual router group, then override the configured value by using the ip vrrp group set or ipv6 vrrp group set command with the override option and enable the virtual router group again.
- The VRRP router version (v2 or v3) determines the advertising interval value range and the level of granularity that is used to specify the interval value. For example:
  - The advertising interval range for VRRP version 2 is 1–25500 and cannot be less than 100 centiseconds. The interval value should also be entered in increments of 100 (for example, 100, 200, 300) up to the maximum allowed. If an interval value is not specified in an increment of 100, then the value is rounded down to the next increment of 100. For example, if a value of 209 is specified, then that value is rounded down to 200.
  - The advertising interval range for VRRP version 3 is 1–4095 and cannot be less than 10 centiseconds. The interval value should also be entered in increments of 10 (for example, 10, 20, 30) up to the maximum allowed. If the interval value is not specified in an increment of 10, then the value is rounded down to the next increment of 10. For example, if a value of 15 is specified, then that value is rounded down to 10.
- When a virtual router group is deleted, the virtual routers assigned to the group become unassigned. However, this does not have any impact on the virtual routers.

Examples

-> ip vrrp group 25 interval 200 priority 50 no preempt version v3
-> no ip vrrp group 25

-> ipv6 vrrp group 30 interval 200 priority 75 preempt no accept
-> no ipv6 vrrp group 30

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; accept and version parameters added.
Release 8.7R2; VRRP router advertising interval range updated.
Related Commands

**vrrp group admin-state**  Changes the administrative status of all the virtual routers in a virtual router group using a single command.

**vrrp group set**  Sets the new modified default value to all the virtual routers in a virtual router group.

**vrrp group-association**  Adds a virtual router to a virtual router group.

**show vrrp group**  Displays the default parameter values for all the virtual router groups or a specific virtual router group.

MIB Objects

alaVrrpv3GroupTable
  alaVrrpv3GroupId
  alaVrrpv3GroupInterval
  alaVrrpv3GroupPriority
  alaVrrpv3GroupPreemptMode
  alaVrrpv3GroupAcceptMode
  alaVrrpv3GroupVersion
  alaVrrpv3GroupRowStatus
vrrp group admin-state

Changes the administrative status of all the IPv4 or IPv6 virtual routers in an IPv4 or IPv6 virtual router group using a single command.

{ip | ipv6} vrrp group vrgid admin-state [disable | enable | enable-all]

Syntax Definitions

- **ip**: Changes the administrative status of all IPv4 virtual routers in the IPv4 group.
- **ipv6**: Changes the administrative status of all IPv6 virtual routers in the IPv6 group.
- **vrgid**: The virtual router group ID. The valid range is 1–255.
- **disable**: Disables all the virtual routers in the group.
- **enable**: Enables those virtual routers that have not previously been disabled individually in the group.
- **enable-all**: Enables all the virtual routers in the group including those virtual routers that have been disabled individually.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If an IPv4 or IPv6 virtual router in a group is disabled on an individual basis, it can only be re-enabled by using the **enable-all** option in this command.
- This command will not affect the ability to change the administrative status of an individual IPv4 or IPv6 virtual router.

Examples

- `-> ip vrrp group 25 admin-state disable`
- `-> ip vrrp group 25 admin-state enable`
- `-> ip vrrp group 25 admin-state enable-all`
- `-> ipv6 vrrp group 30 admin-state disable`
- `-> ipv6 vrrp group 30 admin-state enable`
-> ipv6 vrrp group 30 admin-state enable-all

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added.

**Related Commands**

- `vrrp group` Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
- `vrrp group set` Sets the new modified default value to all the virtual routers in a virtual router group.
- `show vrrp` Displays the virtual router configuration for all virtual routers or for a specific virtual router.
- `show vrrp group` Displays the default parameter values for all the virtual router groups or a specific virtual router group.

**MIB Objects**

alaVrrpv3GroupTable
  alaVrrpv3GroupAdminState
**vrrp group set**

Applies the group default parameter values to all virtual routers in an IPv4 or IPv6 virtual router group. When this command is used, IPv4 or IPv6 virtual routers revert to using the group default parameter values.

```
{ip | ipv6} vrrp group vrgid set [interval | priority | preempt | accept | version | all] [override]
```

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Applies the default parameter values to IPv4 virtual routers.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Applies the default parameter values to IPv6 virtual routers.</td>
</tr>
<tr>
<td>vrgid</td>
<td>The virtual router group ID, in the range from 1–255.</td>
</tr>
<tr>
<td>interval</td>
<td>Sets the VRRP advertisement interval value to the default value.</td>
</tr>
<tr>
<td>priority</td>
<td>Sets the priority value to the default value.</td>
</tr>
<tr>
<td>preempt</td>
<td>Sets the preempt mode to the default mode.</td>
</tr>
<tr>
<td>accept</td>
<td>Sets the accept mode to the default mode.</td>
</tr>
<tr>
<td>version</td>
<td>Sets the VRRP version for IPv4 virtual routers to the default value.</td>
</tr>
<tr>
<td>all</td>
<td>Sets all the parameters’ value to the new default value.</td>
</tr>
<tr>
<td>override</td>
<td>Overrides the configured parameter value with the group default value.</td>
</tr>
</tbody>
</table>

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval</td>
<td></td>
</tr>
<tr>
<td>priority</td>
<td></td>
</tr>
<tr>
<td>preempt</td>
<td></td>
</tr>
<tr>
<td>accept</td>
<td></td>
</tr>
<tr>
<td>version</td>
<td></td>
</tr>
<tr>
<td>all</td>
<td></td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- All the virtual routers in an IPv4 or IPv6 group must be disabled before using this command.
- To apply the group default value to the virtual routers in a group, first disable the virtual router group, then apply the group default value using the `ip vrrp group set` or `ipv6 vrrp group set` command and enable the virtual router group again.
- If any of the virtual routers in the group are running with their own configured parameter value, then that value will take priority over the group default value. To override the configured value with the
group default value, first disable the virtual router group, then override the configured value by using the `ip vrrp group set` or `ipv6 vrrp group set` command with the `override` option and enable the virtual router group again.

**Examples**

- `ip vrrp group 10 admin-state disable`
- `ip vrrp group 10 set priority`
- `ip vrrp group 10 set priority override`
- `ip vrrp group 10 admin-state disable`

- `ipv6 vrrp group 20 admin-state disable`
- `ipv6 vrrp group 20 set interval`
- `ipv6 vrrp group 20 set interval override`
- `ipv6 vrrp group 20 admin-state enable`

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; **accept** and **version** parameters added.

**Related Commands**

- `vrrp group` Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
- `vrrp group admin-state` Changes the administrative status of all the virtual routers in a virtual router group using a single command.
- `show vrrp` Displays the virtual router configuration for all virtual routers or for a specific virtual router.
- `show vrrp group` Displays the default parameter values for all the virtual router groups or a specific virtual router group.

**MIB Objects**

- `alaVrrpv3GroupTable`
  - `alaVrrpv3GroupSetParam`
  - `alaVrrpv3GroupOverride`
vrrp group-association

Adds an IPv4 or IPv6 virtual router to an IPv4 or IPv6 virtual router group.

```
{ip | ipv6} vrrp vrid interface if_name group-association vrgid
{ip | ipv6} vrrp vrid interface if_name no group-association vrgid
```

Syntax Definitions

- **ip**: Adds an IPv4 virtual router to an IPv4 virtual router group.
- **ipv6**: Adds an IPv6 virtual router to an IPv6 virtual router group.
- **vrid**: The virtual router ID. The valid range is 1–255.
- **if_name**: The name of an existing IPv4 or IPv6 interface on which the virtual router is configured.
- **vrgid**: An existing virtual router group ID. The valid range is 1–255.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to remove the IPv4 or IPv6 virtual router from the virtual router group.
- It is not necessary to disable an IPv4 or IPv6 virtual router before adding the virtual router to a group. However, the virtual router will not adopt the group’s default parameter values until it is re-enabled.
- It is not necessary to disable an IPv4 or IPv6 virtual router before removing the virtual router from a group.
- Create separate groups for each combination of protocol and version. For example, if IPv4 group 10 specifies VRRP version 2, then only assign IPv4 version 2 virtual routers to group 10.
  - The first virtual router assigned to the group will determine the protocol and version of the group.
  - IPv6 virtual router groups will always be version 3.
  - IPv4 version 3 virtual routers cannot be assigned to a version 2 group and vice versa. However, the version for an IPv4 group can be changed.
**Examples**

-> ip vrrp 25 interface ipv4-100 group-association 10  
-> ip vrrp 25 interface ipv4-100 no group-association 10  
-> ipv6 vrrp 30 interface ipv6-200 group-association 20  
-> ipv6 vrrp 30 interface ipv6-200 no group-association 20

**Release History**

Release 7.1.1; command was introduced.  
Release 8.5R2; IPv6 virtual router support and `interface` parameter added; `vlan_id` parameter deprecated.

**Related Commands**

`show vrrp group-association` Displays the virtual routers that are associated with a group.

**MIB Objects**

alaVrrpv3AssoGroupTable  
alaVrrpv3AssoGroupRowStatus
**show vrrp**

Displays the virtual router configuration for all virtual routers or for a specific virtual router.

```
show {ip | ipv6} vrrp [vrid]
```

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>IP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Displays the IPv4 virtual router configuration.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Displays the IPv6 virtual router configuration.</td>
</tr>
<tr>
<td>vrid</td>
<td>The virtual router ID, in the range from 1–255.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `show ip vrrp` command to display information about configuration parameters, which may be set through the `ip vrrp` command. Use the `show ip vrrp statistics` command to get information about IPv4 VRRP packets.

- Use the `show ipv6 vrrp` command to display information about configuration parameters, which may be set through the `ipv6 vrrp` command. Use the `show ipv6 vrrp statistics` command to get information about IPv6 VRRP packets.

**Examples**

```
-> show ip vrrp
VRRP default advertisement interval: 100 centiseconds
VRRP default priority: 100
VRRP default preempt: Yes
VRRP default accept: Yes
VRRP default version: V2
VRRP startup delay: 45 (expired)
VRRP BFD-STATE : Disabled

<table>
<thead>
<tr>
<th>VRID</th>
<th>Name</th>
<th>IPv4 Address(es)</th>
<th>Admin Version</th>
<th>Status</th>
<th>Priority</th>
<th>Preempt</th>
<th>Accept</th>
<th>Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>ipv4-100</td>
<td>192.60.170.2</td>
<td>V2</td>
<td>Disabled</td>
<td>100</td>
<td>Yes</td>
<td>NA</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.60.170.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
VRRP Commands

```
20 ipv4-200 30.3.3.1 V2 Enabled 100 Yes NA 100
-> show ip vrrp 10
Virtual Router VRID = 10 on INTERFACE = ipv4-100
  Version = V2
  Admin. Status = Disabled
  Priority = 100
  Preempt = Yes
  Adv. Interval = 100
  Virtual MAC = 00-00-5E-00-01-0A
  IP Address(es)
    192.60.170.2
    192.60.170.3

-> show ipv6 vrrp
VRRP default advertisement interval: 100 centiseconds
VRRP default priority: 100
VRRP default preempt: Yes
VRRP default accept: Yes
VRRP startup delay: 50  (expired)
VRRP BFD-STATE : Disabled

Interface                         Admin                              Adv.
VRID      Name    IPv6 Address(es)        Status   Priority Preempt Accept Interval
----+------------+-----------------------+--------+--------+-------+------+--------
1  ipv6-100     fe80::200:5eff:fe00:201  Enabled      100     Yes    Yes      100
2  ipv6-200     fe80::200:5eff:fe00:202  Enabled      100     Yes    Yes      100
3  ipv6-300     fe80::200:5eff:fe00:203  Enabled      100     Yes    Yes      100
4  ipv6-400     fe80::200:5eff:fe00:204  Enabled      100     Yes    Yes      100

-> show ipv6 vrrp 3
Virtual Router VRID = 3 on INTERFACE = ipv6-300
  Version = V3
  Admin. Status = Enabled
  Priority = 100
  Preempt = Yes
  Accept = Yes
  Adv. Interval = 100
  Virtual MAC = 00-00-5E-00-02-36
  IP Address(es)
    fe80::200:5eff:fe00:203
```

output definitions

VRRP default advertisement interval
The default advertising interval for all virtual routers on the switch.
Configured through the `vrrp interval` command.

VRRP default priority
The default priority value for all virtual routers on the switch.
Configured through the `vrrp priority` command.

VRRP default preempt
The default preempt mode for all virtual routers on the switch.
Configured through the `vrrp preempt` command.

VRRP default accept
The default accept mode for all virtual routers on the switch.
Configured through the `vrrp accept` command.

VRRP default version
The default VRRP version assigned to all IPv4 virtual routers. IPv6 virtual routers support only version 3. Configured through the `vrrp version` command.
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP startup delay</td>
<td>The amount of time after a reboot that virtual routers will wait before they go active; allows time for routing tables to stabilize. Configured through the <code>vrrp delay</code> command.</td>
</tr>
<tr>
<td>VRRP BFD-STATUS</td>
<td>Indicates whether or not (Enabled or Disabled) VRRP is registered to interact with the Bidirectional Forwarding Detection (BFD) protocol. Configured through the <code>vrrp bfd-state</code> command.</td>
</tr>
<tr>
<td>VRID</td>
<td>Virtual router identifier. Configured through the <code>vrrp</code> command.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The IPv4 or IPv6 interface associated with the VRRP instance. Configured through the <code>vrrp</code> command.</td>
</tr>
<tr>
<td>IPv4 Address(es)</td>
<td>The assigned IPv4 or IPv6 addresses. Configured through the <code>vrrp address</code> command.</td>
</tr>
<tr>
<td>IPv6 Address(es)</td>
<td>The assigned IPv4 or IPv6 addresses. Configured through the <code>vrrp address</code> command.</td>
</tr>
<tr>
<td>Version</td>
<td>The VRRP version assigned to the virtual router (V2 or V3). Configured for IPv4 virtual routers through the <code>vrrp</code> command. This value is always set to V3 for IPv6 virtual routers.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The administrative status of this virtual router instance (Enabled allows the virtual router instance to operate; Disabled disables the virtual router instance without deleting it). Configured through the <code>vrrp</code> command.</td>
</tr>
<tr>
<td>Priority</td>
<td>Indicates the VRRP router’s priority for the virtual router. Configured through the <code>vrrp</code> command.</td>
</tr>
<tr>
<td>Preempt</td>
<td>Indicates whether or not (Yes or No) a higher priority virtual router will preempt a lower priority master router: preempt indicates that a higher priority virtual router will preempt a lower priority master; no preempt indicates that the first backup router to take over for the master will not be preempted by a virtual router with a higher priority. In either case, the IP address owner will always take over it if is available. Configured through the <code>vrrp</code> command.</td>
</tr>
<tr>
<td>Accept</td>
<td>Indicates whether or not (Yes or No) a master router that is not the IP address owner will accept packets addressed to the IP address owner as its own. Configured through the <code>vrrp</code> command. This parameter applies only to IPv4 version 3 and IPv6 virtual routers.</td>
</tr>
<tr>
<td>Adv. Interval</td>
<td>Indicates the time interval (in centiseconds) between sending advertisement messages. Only the master router sends advertisements. Configured through the <code>vrrp</code> command.</td>
</tr>
<tr>
<td>Virtual MAC</td>
<td>Displays the virtual MAC address for the virtual router.</td>
</tr>
</tbody>
</table>

- The first 5 bytes for IPv4 and IPv6 version 3 virtual routers is always 00-00-5E-00-02.
- The first 5 bytes for IPv4 version 2 virtual routers is always 00-00-5E-00-01.
- The last byte indicates the VRID.

Release History

- Release 7.1.1; command was introduced.
- Release 8.5R2; “VLAN” field replaced with “Interface Name” field; “Accept” and “Version” fields added.
Related Commands

**show vrrp statistics**  Displays statistics for all virtual routers configured on the switch or for a specific virtual router.

MIB Objects

vrrpv3OperationsTable
  vrrpv3OperationsVrId
  vrrpv3OperationsInetAddrType
  vrrpv3OperationsMasterIpAddr
  vrrpv3OperationsRowStatus
  vrrpv3OperationsPriority
  vrrpv3OperationsPreemptMode
  vrrpv3OperationsAcceptMode
  vrrpv3OperationsAdvInterval
alaVrrpv3OperationsExTable
  alaVrrpv3OperVersion
**show vrrp statistics**

Displays statistics about VRRP packets for all virtual routers configured on the switch or for a specific virtual router.

```
show {ip | ipv6} [vrid] statistics
```

**Syntax Definitions**

- **ip**
  - Displays VRRP packet statistics for IPv4 virtual routers.
- **ipv6**
  - Displays VRRP packet statistics for IPv6 virtual routers.
- **vrid**
  - The virtual router ID. The valid range is 1–255.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **show ip vrrp statistics** command to display information about IPv4 VRRP packets. Use the **show ip vrrp** command to display information about the IPv4 virtual router configuration.
- Use the **show ipv6 vrrp statistics** command to display information about IPv6 VRRP packets. Use the **show ipv6 vrrp** command to display information about the IPv6 virtual router configuration.

**Examples**

```
-> show ip vrrp statistics
Checksum Errors :          0,
Version Errors  :          0,
VRID Errors     :          0

Interface
VRID     Name     State     UpTime   Become Master     Adv. Rcvd
---------+----------+----------+----------+-------------------+----------
 1       ipv4-100 Master   378890   1          0
 2       ipv4-15   Backup   4483     0          44
 7       ipv4-200 Initialize 0         0          0
```
-> show ipv6 vrrp statistics
Checksum Errors :          0,
Version Errors  :          0,
VRID Errors     :          0

<table>
<thead>
<tr>
<th>Interface</th>
<th>VRID</th>
<th>Name</th>
<th>State</th>
<th>UpTime</th>
<th>Become Master</th>
<th>Adv. Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ipv6-101</td>
<td>Master</td>
<td>2983</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>ipv6-102</td>
<td>Master</td>
<td>60675</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>ipv6-103</td>
<td>Master</td>
<td>60675</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

output definitions

Checksum Errors
The total number of VRRP packets received with an invalid checksum value.

Version Errors
The total number of VRRP packets received with an invalid version number.

VRID Errors
The total number of VRRP packets received with invalid VRIDs.

VRID
The virtual router identifier.

Interface Name
The name of the IPv4 or IPv6 interface associated with the VRRP instance.

State
The operational state of the VRRP router instance:
- initialize—the interface is either disabled or down, or the startup delay timer has not expired.
- backup—this instance is monitoring the availability and state of the master router.
- master—this instance is functioning as the master router.

UpTime
Time interval (in hundredths of a second) since this virtual router was last initialized.

Become Master
The total number of times this virtual router’s state has transitioned from backup to master.

Adv. Rcvd
The total number of VRRP advertisements received by this instance.

-> show ip vrrp 1 statistics
Virtual Router VRID = 1 on INTERFACE = ipv4-100,
State = Master,
UpTime (1/100th second) = 378890,
Become master = 1,
Advertisements received = 0,
Type errors = 0,
Advertisement interval errors = 0,
IP TTL errors = 0,
IP address list errors = 0,
Packet length errors = 0,
Zero priority advertisements sent = 0,
Zero priority advertisements received = 0,
New Master Reason = 0,
Protocol Error Reason = 0,
Discontinuity Time = 0,
Refresh Rate (milliseconds) = 1000
-> show ipv6 vrrp 5 statistics
Virtual Router VRID = 3 on INTERFACE = ipv6-103,
  State = Master,
  UpTime (1/100th second) = 60675,
  Become master = 1,
  Advertisements received = 0,
  Type errors = 0,
  Advertisement interval errors = 0,
  IP TTL errors = 0,
  IP address list errors = 0,
  Packet length errors = 0,
  Zero priority advertisements sent = 0,
  Zero priority advertisements received = 0,
  New Master Reason = 0,
  Protocol Error Reason = 0,
  Discontinuity Time = 0,
  Refresh Rate (milliseconds) = 1000

output definitions

<table>
<thead>
<tr>
<th>VRID</th>
<th>The virtual router identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERFACE</td>
<td>The name of the IPv4 or IPv6 interface associated with the VRRP instance.</td>
</tr>
<tr>
<td>State</td>
<td>The operational state of the VRRP router instance:</td>
</tr>
<tr>
<td></td>
<td>• initialize—the interface is either disabled or down, or the startup delay timer has not expired.</td>
</tr>
<tr>
<td></td>
<td>• backup—this instance is monitoring the availability of the master router.</td>
</tr>
<tr>
<td></td>
<td>• master—this instance is functioning as the master router.</td>
</tr>
<tr>
<td>UpTime</td>
<td>Time interval (in hundredths of a second) since this virtual router was last initialized.</td>
</tr>
<tr>
<td>Become master</td>
<td>The total number of times this virtual router’s state has transitioned from backup to master.</td>
</tr>
<tr>
<td>Advertisements received</td>
<td>The total number of VRRP advertisement packets received by this instance.</td>
</tr>
<tr>
<td>Type errors</td>
<td>The total number of VRRP packets received with an invalid value in the VRRP type field.</td>
</tr>
<tr>
<td>Advertisement interval errors</td>
<td>The total number of VRRP packets received in which the advertisement interval differs from the one configured for the virtual router.</td>
</tr>
<tr>
<td>IP TTL errors</td>
<td>The total number of VRRP packets received with a TTL (Time-To-Live) value other than 255.</td>
</tr>
<tr>
<td>IP address list errors</td>
<td>The total number of VRRP packets in which the IP address list does not match the configured list for the virtual router.</td>
</tr>
<tr>
<td>Packet length errors</td>
<td>The total number of VRRP packets received with a length less than the length of the VRRP header.</td>
</tr>
<tr>
<td>Zero priority advertisements sent</td>
<td>The total number of VRRP advertisements with a priority of 0 sent by the virtual router.</td>
</tr>
<tr>
<td>Zero priority advertisements received</td>
<td>The total number of VRRP advertisements with a priority of 0 received by the virtual router.</td>
</tr>
</tbody>
</table>
VRRP Commands

output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Master Reason</td>
<td>The reason the virtual router transitioned to master state. A value of 0 indicates that the virtual router never transitioned to a master state.</td>
</tr>
<tr>
<td>Protocol Error Reason</td>
<td>The reason for the last protocol error. A value of 0 indicates that no protocol errors have occurred.</td>
</tr>
<tr>
<td>Discontinuity Time</td>
<td>Indicates what the system up time value was when one or more of the statistics counters experienced a discontinuity. A value of 0 indicates that no discontinuities have occurred since the last reboot.</td>
</tr>
<tr>
<td>Refresh Rate (milliseconds)</td>
<td>The minimum polling time interval required to update statistics counters.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; “VLAN” field replaced with “Interface Name” field; “New Master Reason”, “Protocol Error Reason”, “Discontinuity Time”, and “Refresh Rate” fields added.

Related Commands

vrrp
Configures a new VRRP virtual router or modifies an existing one. Used to enable to disable a virtual router.

show vrrp
Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

vrrpv3OperationsTable
  vrrpv3OperationsVrId
  vrrpv3OperationsInetAddrType
  vrrpv3OperationsStatus
  vrrpv3OperationsUpTime

vrrpv3Statistics
  vrrpv3RouterChecksumErrors
  vrrpv3RouterVersionErrors
  vrrpv3RouterVrIdErrors

vrrpv3StatisticsTable
  vrrpv3StatisticsMasterTransitions
  vrrpv3StatisticsRcvdAdvertisements
  vrrpv3StatisticsAdvIntervalErrors
  vrrpv3StatisticsIpTtlErrors
  vrrpv3StatisticsRcvdPriZeroPackets
  vrrpv3StatisticsSentPriZeroPackets
  vrrpv3StatisticsRcvdInvalidTypePackets
  vrrpv3StatisticsAddressListErrors
  vrrpv3StatisticsPacketLengthErrors
  vrrpv3StatisticsNewMasterReason
  vrrpv3StatisticsProtoErrReason
  vrrpv3StatisticsRowDiscontinuityTime
  vrrpv3StatisticsRefreshRate
**show vrrp track**

Displays information about tracking policies on the switch.

show ip vrrp track [track_id]

---

**Syntax Definitions**


track_id

The ID of the tracking policy to display.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Enter the tracking ID to display information about a particular policy; if no tracking policy ID is entered, information for all tracking policies is displayed.

---

**Examples**

```shell
-> show ip vrrp track
Track ID  Policy             Admin  Oper  Pri  BFD
---------+---------------------------+-------+-------+-----+-------+
  1      | PORT 1/1/1                 | Enabled|Up     | 25  | Enabled|
  2      | 192.10.150.42              | Enabled|Down   | 25  | Disabled|
  3      | INTF02-01                  | Enabled|Up     | 25  | Enabled|
```

```shell
-> show ip vrrp track 2
Tracking Policy TRACKID = 2
  Policy = 192.10.150.42
  Dec. Priority = 25
  Admin. Status = Enabled
  Oper. Status = Down
  BFD Status = Disabled
  Delay: 0
```

---

**output definitions**

<table>
<thead>
<tr>
<th></th>
<th>The ID of the tracking policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track ID</td>
<td>The IP interface, chassis/slot/port, or IP address tracked by the policy.</td>
</tr>
</tbody>
</table>
### Release History

Release 7.1.1; command was introduced.
Release 8.4.1; Delay field added.

### Related Commands

- **vrrp track**
  Creates a new tracking policy or modifies an existing tracking policy.

- **show vrrp track-association**
  Displays the tracking policies associated with virtual routers

### MIB Objects

- alaVRRPTrackTable
  - alaVrrpTrackId
  - alaVrrpTrackAdminState
  - alaVrrpTrackPriority
  - alaVrrpTrackState
  - alaVrrpTrackEntityPort
  - alaVrrpTrackEntityIpAddrType
  - alaVrrpTrackEntityIpAddr
  - alaVrrpTrackEntityInterface
  - alaVrrpTrackEntityIpv6Interface
  - alaVrrpTrackBfdStatus
  - alaVrrpTrackDelay

---

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec. Priority</td>
<td>The value to be decremented from the priority value of the virtual router monitoring this tracking policy when the operational state of the tracking policy is down.</td>
</tr>
<tr>
<td>Admin. Status</td>
<td>Whether the tracking policy is administratively Enabled or Disabled.</td>
</tr>
<tr>
<td>Oper. Status</td>
<td>Indicates whether the operating state of the tracking policy is Up or Down.</td>
</tr>
<tr>
<td>BFD Status</td>
<td>The status (Enabled or Disabled) of Bidirectional Forwarding Detection (BFD) interaction with the VRRP tracking policy.</td>
</tr>
<tr>
<td>Delay</td>
<td>The amount of time, in seconds, to wait after a VRRP address track is detected as operationally up and before the associated virtual router's priority value is incremented by the tracking policy's priority value.</td>
</tr>
</tbody>
</table>
**show vrrp track-association**

Displays the tracking policies associated with virtual routers.

`show {ip | ipv6} [vrid] track-association [track_id]`

### Syntax Definitions

- **ip**
  - Displays the tracking policies associated with IPv4 virtual routers.

- **ipv6**
  - Displays the tracking policies associated with IPv6 virtual routers.

- **vrid**
  - The virtual router ID. The valid range is 1–255.

- **track_id**
  - The ID of the tracking policy to display.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 C32E/T24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7200</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If a track ID is specified, only information about that track ID is displayed. If the virtual router ID and track ID are not specified, information about all virtual routers and their associated tracking policies is displayed.

### Examples

```
-> show ip vrrp track-association
VRID Interface Conf Cur Pri Pri ID Policy Admin State Oper State Track Pri
VRID IP Name Pri Pri ID Policy
1  IPV4-100 200 175  1 192.168.170.1 Enabled Up 10
3 INTF02-01  192.168.170.1 Enabled Down 25
2  IPV4-200 200 200  1 192.168.170.1 Enabled Up 10

-> show ip vrrp 1 track-association
VRID Interface Conf Cur Track Policy Admin State Oper State Track Pri
VRID IP Name Pri Pri ID Policy
1  IPV4-100 200 175  1 192.168.170.1 Enabled Up 10
3 INTF02-01  192.168.170.1 Enabled Down 25
```
-> show ip vrrp track-association 1

<table>
<thead>
<tr>
<th>VRID</th>
<th>Name</th>
<th>Pri</th>
<th>Pri</th>
<th>ID</th>
<th>Policy</th>
<th>State</th>
<th>State</th>
<th>Pri</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>IPV4-100</td>
<td>200</td>
<td>175</td>
<td>1</td>
<td>192.168.170.1</td>
<td>Enabled</td>
<td>Up</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>IPV4-200</td>
<td>200</td>
<td>200</td>
<td>1</td>
<td>192.168.170.1</td>
<td>Enabled</td>
<td>Up</td>
<td>10</td>
</tr>
</tbody>
</table>

-> show ipv6 vrrp track-association

<table>
<thead>
<tr>
<th>VRID</th>
<th>Name</th>
<th>Pri</th>
<th>Pri</th>
<th>ID</th>
<th>Policy</th>
<th>State</th>
<th>State</th>
<th>Pri</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ipv6-250</td>
<td>101</td>
<td>200</td>
<td>1</td>
<td>PORT 1/1/37</td>
<td>Enabled</td>
<td>Up</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>ipv6-300</td>
<td>100</td>
<td>100</td>
<td>2</td>
<td>INTFO2-02</td>
<td>Enabled</td>
<td>Up</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>10.255.11.101</td>
<td></td>
<td>Enabled</td>
<td>Up</td>
<td>25</td>
</tr>
</tbody>
</table>

-> show ipv6 vrrp 2 track-association

<table>
<thead>
<tr>
<th>VRID</th>
<th>Name</th>
<th>Pri</th>
<th>Pri</th>
<th>ID</th>
<th>Policy</th>
<th>State</th>
<th>State</th>
<th>Pri</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ipv6-300</td>
<td>100</td>
<td>100</td>
<td>2</td>
<td>INTFO2-02</td>
<td>Enabled</td>
<td>Up</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>10.255.11.101</td>
<td></td>
<td>Enabled</td>
<td>Up</td>
<td>25</td>
</tr>
</tbody>
</table>

-> show ipv6 vrrp track-association 3

<table>
<thead>
<tr>
<th>VRID</th>
<th>Name</th>
<th>Pri</th>
<th>Pri</th>
<th>ID</th>
<th>Policy</th>
<th>State</th>
<th>State</th>
<th>Pri</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ipv6-300</td>
<td>100</td>
<td>100</td>
<td>3</td>
<td>10.255.11.101</td>
<td>Enabled</td>
<td>Up</td>
<td>25</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID</td>
<td>The virtual router identifier.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The name of the IPv4 or IPv6 interface associated with the virtual router.</td>
</tr>
<tr>
<td>Conf Pri</td>
<td>The priority configured for the virtual router.</td>
</tr>
<tr>
<td>Cur Pri</td>
<td>The current priority for the virtual router. If the tracking policy is in effect because the tracked entity is down, the current priority will be equal to the configured priority (Conf Pri) minus the tracking priority (Track Pri). Otherwise, the current priority will be equal to the configured priority.</td>
</tr>
<tr>
<td>Track ID</td>
<td>The ID of the tracking policy.</td>
</tr>
<tr>
<td>Policy</td>
<td>The IPv4 interface, IPv6 interface, port, IPv4 address, or IPv6 address that this policy is tracking.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The administrative status (Enabled or Disabled) of the tracking policy.</td>
</tr>
<tr>
<td>Oper State</td>
<td>The operational status (Up or Down) of the tracking policy.</td>
</tr>
<tr>
<td>Track Pri</td>
<td>The amount to be decremented from the configured virtual router priority when the tracking policy is applied.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; “VLAN” field replaced with “Interface Name” field.
Related Commands

**vrrp track-association**
Associates a VRRP tracking policy with a virtual router.

**vrrp track**
Creates a new tracking policy or modifies an existing tracking policy.

**show vrrp track**
Displays information about tracking policies on the switch

**show vrrp**
Displays the virtual router configuration for all virtual routers or for a specific virtual router.

MIB Objects

vrrpOperTable
- vrrpOperPriority
vrrpv3OperationsTable
- vrrpv3OperationsVrId
- vrrpv3OperationsInetAddrType
alaVrrpv3OperationsExTable
- alaVrrpv3CurrentPriority
alaVrrpAssoTrackTable
- alaVrrpAssoTrackId
alaVRRPTrackTable
- alaVrrpTrackId
- alaVrrpTrackAdminState
- alaVrrpTrackPriority
- alaVrrpTrackState
- alaVrrpTrackEntityPort
- alaVrrpTrackEntityIpAddrType
- alaVrrpTrackEntityIpAddr
- alaVrrpTrackEntityInterface
- alaVrrpTrackEntityIpv6Interface
show vrrp group

Displays the default parameter values for all the virtual router groups or for a specific virtual router group.

show {ip | ipv6} vrrp group [vrgid]

Syntax Definitions

*ip* Displays the IPv4 virtual routers that belong to a group.

*ipv6* Displays the IPv6 virtual routers that belong to a group.

*vrgid* The virtual router group ID, in the range from 1–255.

Defaults

By default, the default parameter values are displayed for all the virtual router groups.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the *vrgid* parameter with this command to display the default values for a specific virtual router group.

Examples

```bash
-> show ip vrrp group
Group    Adv     Preempt   Accept
ID  Interval Priority Mode   Mode   Version
-------+--------+----------+--------+--------+-------
10     200    75       Yes    No     V3
20     150    75       Yes    No     V2

-> show ip vrrp group 20
Virtual Router Group GROUPID = 20
  Interval = 150
  Priority = 75
  Preempt Mode = Yes
  Accept Mode = No
  Version = V2
  2 Associated Virtual Routers

-> show ipv6 vrrp group
Group      Adv     Preempt   Accept
ID  Interval Priority Mode   Mode   Version
-------+--------+----------+--------+--------+-------
```
show vrrp group

```
--+--------+----------+--------+--------+-------
|30| 100    | 75       | Yes    | No    | V3    |
|40| 125    | 75       | Yes    | Yes   | V3    |
```

`-> show ipv6 vrrp group 30
Virtual Router Group GROUPID = 30
   Interval = 100
   Priority = 75
   Preempt Mode = Yes
   Accept Mode = No
   Version = V3
   2 Associated Virtual Routers

**output definitions**

<table>
<thead>
<tr>
<th>Group ID</th>
<th>The virtual router group identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adv Interval</td>
<td>The default advertisement time interval, in centiseconds, for the VRRP group. Only the master router sends advertisements.</td>
</tr>
<tr>
<td>Priority</td>
<td>The default priority value for the VRRP group.</td>
</tr>
<tr>
<td>Preempt Mode</td>
<td>The default preempt mode (Yes or No) for the VRRP group.</td>
</tr>
<tr>
<td>Accept Mode</td>
<td>The default accept mode (Yes or No) for the VRRP group.</td>
</tr>
<tr>
<td>Version</td>
<td>The default VRRP version (V2 or V3) for an IPv4 VRRP group. IPv6 virtual routers support only version 3, so IPv6 VRRP groups are automatically set to V3.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; “Accept Mode” and “Version” parameters added.

**Related Commands**

- `vrrp group` Creates a new virtual router group or modifies the configuration parameters of an existing virtual router group.
- `vrrp group admin-state` Changes the administrative status of all the virtual routers in a virtual router group using a single command.

**MIB Objects**

- `alaVrrpv3GroupTable`
  - `alaVrrpv3GroupId`
  - `alaVrrpv3GroupInterval`
  - `alaVrrpv3GroupPriority`
  - `alaVrrpv3GroupPreemptMode`
  - `alaVrrpv3GroupAcceptMode`
  - `alaVrrpv3GroupVersion`
**show vrrp group-association**

Displays the virtual routers that are associated with a virtual router group.

**show {ip | ipv6} vrrp group-association [vrgid]**

---

**Syntax Definitions**

- **ip**: Displays the IPv4 virtual routers that belong to a group.
- **ipv6**: Displays the IPv6 virtual routers that belong to a group.
- **vrgid**: The virtual router group ID, in the range from 1–255.

**Defaults**

By default, all virtual router group associations are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Command Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **vrgid** parameter with this command to display the association details of a specific virtual router group.

**Examples**

```
-> show ip vrrp group-association
Interface
GROUPID VRID   Name                Version
--------------------------------------------
 10   5  ipv4-100                            V2
     6  ipv4-200                            V2
 20   21  ipv4-300                            V3
     22  ipv4-400                            V3

-> show ip vrrp group-association 20
Interface
GROUPID VRID   Name                Version
--------------------------------------------
 20   21  ipv4-300                            V3
     22  ipv4-400                            V3
```
VRRP Commands

show vrrp group-association

-> show ipv6 vrrp group-association

<table>
<thead>
<tr>
<th>GROUPID</th>
<th>VRID</th>
<th>Interface</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>31</td>
<td>ipv6-500</td>
<td>V3</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>ipv6-600</td>
<td>V3</td>
</tr>
<tr>
<td>40</td>
<td>41</td>
<td>ipv6-700</td>
<td>V3</td>
</tr>
<tr>
<td>42</td>
<td></td>
<td>ipv6-800</td>
<td>V3</td>
</tr>
</tbody>
</table>

-> show ipv6 vrrp group-association 30

<table>
<thead>
<tr>
<th>GROUPID</th>
<th>VRID</th>
<th>Interface</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>31</td>
<td>ipv6-500</td>
<td>V3</td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>ipv6-600</td>
<td>V3</td>
</tr>
</tbody>
</table>

output definitions

| GROUPID | The virtual router group identifier.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID</td>
<td>The virtual router identifier.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The IPv4 or IPv6 interface associated with the VRRP instance.</td>
</tr>
<tr>
<td>Version</td>
<td>The VRRP version for the group (V2 or V3)</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.5R2; IPv6 virtual router support added; “Interface Name” and “Version” fields added; “VLAN” field deprecated.

Related Commands

vrrp group-association Adds a virtual router to a virtual router group.

MIB Objects

alaVrrpAssoGroupTable
alaVrrpGroupIdent
ifIndex
vrrpOperVrId
alaVrrpv3AssoGroupTable
alaVrrpv3GroupIdent
vrrpv3OperationsInetAddrType
ifIndex
vrrpv3OperationsVrId
27 OSPF Commands

Open Shortest Path First routing (OSPF) is a shortest path first (SPF) or link-state protocol. OSPF is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPF chooses the least-cost path as the best path.

Each participating router distributes its local state (i.e., the router’s usable interfaces and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. This database is built from the collected link state advertisements of all routers. Each multi-access network that has at least two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities.

OSPF allows collections of contiguous networks and hosts to be grouped together. A group, together with the routers having interfaces to any one of the included networks, is called an area. Each area runs a separate copy of the basic link-state routing algorithm. This means that each area has its own topological database, as explained in the previous section.

The OmniSwitch version of OSPF complies with RFCs 1370, 1850, 2328, 2370, 3101, and 3623.

MIB information for OSPF is as follows:

- **Filename**: ALCATEL-IND1-VIRTUALROUTER-MIB.mib
  - **Module**: alcatelIND1VirtualRouterMIB

- **Filename**: ALCATEL-IND1-OSPF-MIB.mib
  - **Module**: alcatelIND1OSPFMIB

- **Filename**: OSPF-MIB.mib
  - **Module**: OSPF
The following is a list of the commands for configuring OSPF:

<table>
<thead>
<tr>
<th>Category</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global OSPF Commands</strong></td>
<td>ip load ospf&lt;br&gt;ip ospf admin-state&lt;br&gt;ip ospf asbr&lt;br&gt;ip ospf exit-overflow-interval&lt;br&gt;ip ospf extlsdb-limit&lt;br&gt;ip ospf host&lt;br&gt;ip ospf mtu-checking&lt;br&gt;ip ospf default-originate&lt;br&gt;ip ospf route-tag&lt;br&gt;ip ospf spf-timer&lt;br&gt;ip ospf virtual-link&lt;br&gt;ip ospf neighbor&lt;br&gt;ip ospf redist-bgp-internal&lt;br&gt;show ip ospf&lt;br&gt;show ip ospf border-routers&lt;br&gt;show ip ospf ext-lsdb&lt;br&gt;show ip ospf host&lt;br&gt;show ip ospf lsdb&lt;br&gt;show ip ospf neighbor&lt;br&gt;show ip ospf routes&lt;br&gt;show ip ospf virtual-link&lt;br&gt;show ip ospf virtual-neighbor</td>
</tr>
<tr>
<td><strong>OSPF Area Commands</strong></td>
<td>ip ospf area&lt;br&gt;ip ospf area default-metric&lt;br&gt;ip ospf area range&lt;br&gt;show ip ospf area&lt;br&gt;show ip ospf area range&lt;br&gt;show ip ospf area stub</td>
</tr>
<tr>
<td><strong>OSPF Interface Commands</strong></td>
<td>ip ospf interface&lt;br&gt;ip ospf interface admin-state&lt;br&gt;ip ospf interface area&lt;br&gt;ip ospf interface auth-key&lt;br&gt;ip ospf interface auth-type&lt;br&gt;ip ospf interface dead-interval&lt;br&gt;ip ospf interface hello-interval&lt;br&gt;ip ospf interface md5&lt;br&gt;ip ospf interface md5 key&lt;br&gt;ip ospf interface type&lt;br&gt;ip ospf interface cost&lt;br&gt;ip ospf interface poll-interval&lt;br&gt;ip ospf interface priority&lt;br&gt;ip ospf interface retrans-interval&lt;br&gt;ip ospf interface transit-delay&lt;br&gt;show ip ospf interface&lt;br&gt;show ip ospf interface auth-info</td>
</tr>
<tr>
<td><strong>OSPF BFD Commands</strong></td>
<td>ip ospf bfd-state&lt;br&gt;ip ospf bfd-state all-interfaces&lt;br&gt;ip ospf interface bfd-state&lt;br&gt;ip ospf interface bfd-state drs-only&lt;br&gt;ip ospf interface bfd-state all-neighbors</td>
</tr>
<tr>
<td><strong>OSPF Graceful Restart Commands</strong></td>
<td>ip ospf restart-support&lt;br&gt;ip ospf restart-interval&lt;br&gt;ip ospf restart-helper admin-state&lt;br&gt;ip ospf restart-helper strict-lsa-checking admin-state&lt;br&gt;ip ospf restart initiate&lt;br&gt;show ip ospf restart</td>
</tr>
</tbody>
</table>
ip load ospf

Loads the OSPF software on the router.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Example

-> ip load ospf

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

alaVrConfigTable
  alaVrConfigOspfStatus
**ip ospf admin-state**

Enables or disables the administration status of OSPF on the router.

```
ip ospf admin-state {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables OSPF.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables OSPF.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The OSPF protocol must be enabled for it to route traffic.

### Examples

```
-> ip ospf admin-state enable
-> ip ospf admin-state disable
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show ip ospf` Displays OSPF status and general configuration parameters.

### MIB Objects

- `ospfGeneralGroup`
- `ospfAdminStat`
**ip ospf asbr**

Configures the router as an Autonomous System Border Router (ASBR). A router running multiple protocols or acting as a gateway to other exterior routers is an ASBR.

- **ip ospf asbr**
- **no ip ospf asbr**

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- Autonomous System Border Routers (ASBRs) are routers that exchange information with routers from another autonomous system (AS).
- The `no` variant of this command removes the ASBR classification of the selected router.

**Examples**

- `-> ip ospf asbr`
- `-> no ip ospf asbr`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip ospf` Displays OSPF status and general configuration parameters.

**MIB Objects**

- `alaProtocolOspf`
- `alaOspfAsBdRtr`
**ip ospf exit-overflow-interval**

This command sets the overflow interval value.

`ip ospf exit-overflow-interval seconds`

---

**Syntax Definitions**

seconds: The number of seconds the router waits before attempting to leave the overflow state.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The overflow interval is the time whereby the routing router will wait before attempting to leave the database overflow state; the interval begins upon the routing router’s arrival into this state.

- When the routing router leaves the overflow state, it can once again create non-default and external link state advertisements (LSAs) for autonomous systems (AS).

- Note that the router will not leave the overflow state (until it is restarted) when the overflow interval value is set to 0.

---

**Example**

```
-> ip ospf exit-overflow-interval 10
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ip ospf

Displays the OSPF status and general configuration parameters.

MIB Objects

ospfGeneralGroup

ospfExitOverflowInterval
**ip ospf extlsdb-limit**

Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

```
ip ospf extlsdb-limit limit
```

### Syntax Definitions

- **limit**: The maximum number of LSDB entries allowed on the router. The accepted value is any number greater than or equal to 1. If 0 is entered, there is no limit.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>limit</td>
<td>-1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C4E/V48C8/C32E/T24C2/X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command allows you to set a limit to the number of external LSDBs learned by the router. An external LSDB is created when the router learns a link address that exists outside of its Autonomous System (AS).

- When the limit is set, and it is exceeded, older addresses that were previously learned are removed from the routing table to make room for the new external LSDB.

### Example

```
-> ip ospf extlsdb-limit 25
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `show ip ospf` Displays OSPF status and general configuration parameters.

**MIB Objects**

- `ospfGeneralGroup`
- `ospfExtLsdbLimit`
**ip ospf host**

Creates and deletes an OSPF entry for directly attached hosts. Allows for the modification of the host parameters of Type of Service (ToS) and metric.

```
ip ospf host ip_address tos tos [metric metric]
no ip ospf host ip_address tos tos
```

**Syntax Definitions**

- **ip_address**
  - The 32-bit IP address in dotted decimal format of the OSPF host. See the example below for more information.

- **tos**
  - The type of service (ToS) of the specified OSPF host. The valid range is 0-15. Only ToS value 0 is supported at this time.

- **metric**
  - The cost metric value assigned to the specified host. The valid range is 0 and up.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The **no** variant of this command removes the record of the OSPF host.

- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. ToS routing is the ability to make a forwarding decision based on a destination address and a desired Quality of Service (QoS). ToS routing allows link selection based on QoS when more than one path exists between a source and a destination. A metric value is the cost of all the hops necessary for a packet to reach its destination. Routers use the metric to determine the best possible path.

**Examples**

```
-> ip ospf host 172.22.2.115 tos 1 metric 10
-> no ip ospf host 172.22.2.115 tos 1
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`show ip ospf host` Displays information on configured OSPF hosts.

**MIB Objects**

`ospfHostTable`
- `ospfHostStatus`
- `ospfHostIpAddress`
- `ospfHostTOS`
- `ospfHostMetric`
ip ospf mtu-checking

Enables or disables the use of Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

ip ospf mtu-checking
no ip ospf mtu-checking

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
- The no form of this command disables MTU checking.
- This command is used to disable the checking for mismatch of the interface MTU while establishing a neighbor adjacency with a router. MTU mismatch occurs when a router receives packets that contain a larger MTU value than that of the interface on which adjacency is being established. The interface MTU is the largest IP datagram size (in bytes) that the interface can accept.

Examples
- ip ospf mtu-checking
- no ip ospf mtu-checking

Release History
Release 7.1.1; command was introduced.
Related Commands

show ip ospf

Displays the OSPF status and general configuration parameters.

MIB Objects

alaProtocolOspf
alaOspfMTUCheck
**ip ospf default-originate**

Configures a default external route into the OSPF routing domain.

**ip ospf default-originate {only | always} [metric-type {type1 | type2}] [metric value]**

**no ip ospf default-originate**

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>only</td>
<td>Advertises only when there is a default route in the routing table.</td>
</tr>
<tr>
<td>always</td>
<td>Advertises the default route regardless of whether the routing table has a default route.</td>
</tr>
<tr>
<td>type1</td>
<td>Sets the external route as type1.</td>
</tr>
<tr>
<td>type2</td>
<td>Sets the external route as type2.</td>
</tr>
<tr>
<td>value</td>
<td>The metric value. The valid range is 1-65535.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>type1</td>
<td>type2</td>
</tr>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **no** form of the command to delete redistributed default routes.

**Examples**

- `ip ospf default-originate always`
- `ip ospf default-originate only metric 10`
- `ip ospf default-originate always metric-type type1 metric 5`
- `no ip ospf default-originate`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**show ip ospf**
Displays the OSPF status and general configuration parameters.

MIB Objects

alaProtocolOspf

alaOspfDefaultOriginate
alaOspfDefaultOriginateMetricType
alaOspfDefaultOriginateMetric
**ip ospf route-tag**

Configures a tag value that is applied to internal routes for potential redistribution.

**ip ospf route-tag tag**

---

### Syntax Definitions

**tag**

The set tag value. The valid range is 0–2147483647.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>0</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

A 32-bit value tagged to each OSPF internal route that is redistributed into other routing protocol domains. The lower 16-bits typically indicate the autonomous system number.

---

### Example

```
-> ip ospf route-tag 2
```

---

### Release History

Release 7.1.1; command was introduced.

---

### Related Commands

- **show ip ospf**
  
  Displays OSPF status and general configuration parameters.

---

### MIB Objects

- `alaProtocolOspf`
- `alaOspfRedistRouteTag`
ip ospf spf-timer

Configures timers for Shortest Path First (SPF) calculation.

ip ospf spf-timer [delay delay_seconds] [hold hold_seconds]

Syntax Definitions

delay_seconds  
Specifies time (from 0 to 65535 seconds) between the reception of an OSPF topology change and the start of an SPF calculation.

hold_seconds  
 Specifies the minimum time (from 0 to 65535 seconds) between consecutive SPF calculations.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay_seconds</td>
<td>5</td>
</tr>
<tr>
<td>hold_seconds</td>
<td>10</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command allows you to configure the time between SPF calculations. Using the delay timer, you can determine how much time to postpone an SPF calculation after the router receives a topology change. Using the hold timer, you can configure the amount of time that must elapse between consecutive SPF calculations.

- Note that if either of these values is set to 0, there will be no delay in the SPF calculation. This means that SPF calculations will occur immediately upon the reception of a topology change and/or that back-to-back SPF calculations can take place with no break in-between the two.

Example

-> ip ospf spf-timer delay 20 hold 35

Release History

Release 7.1.1; command was introduced.
Related Commands

**show ip ospf**
Displays the OSPF status and general configuration parameters.

MIB Objects

alaProtocolOspf
  - alaOspfTimerSpfDelay
  - alaOspfTimerSpfHold
**ip ospf virtual-link**

Creates or deletes a virtual link. A virtual link is used to restore backbone connectivity if the backbone is not physically contiguous.

```
ip ospf virtual-link area_id router_id [auth-type {none | simple | md5}] [auth-key key_string] [dead-interval seconds] [hello-interval seconds] [retrans-interval seconds] [transit-delay seconds]
```

```
no ip ospf virtual-link area_id router_id
```

### Syntax Definitions

- **area_id**: A unique 32-bit value in IP address format.
- **router_id**: A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
- **none**: Sets the virtual link authorization type to no authentication.
- **simple**: Sets the virtual link authorization type to simple authentication. If `simple` is selected, a key must be specified as well.
- **md5**: Sets the virtual link authorization type to MD5 authentication.
- **key_string**: Sets the virtual link authorization key. The key can be up to 8 ASCII characters. See the example for more details.
- **dead-interval seconds**: Sets the virtual link dead interval. If no hello packets on this link for the set number of seconds have been received, the virtual neighbor is declared dead. The valid range is 1–2147483647.
- **hello-interval seconds**: Sets the virtual link hello interval, which is the time interval between OSPF hellos sent on this virtual link. The valid range is 1–65535.
- **retrans-interval seconds**: Sets the virtual link retransmit interval. The router waits the set number of seconds before retransmitting OSPF packets. The valid range is 0–3600.
- **transit-delay seconds**: Sets the virtual link transit delay, which is the number of seconds to transmit OSPF packets over this link. The valid range is 0–3600.
**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>simple</td>
</tr>
<tr>
<td>key_string</td>
<td>null string</td>
</tr>
<tr>
<td>dead-interval</td>
<td>seconds</td>
</tr>
<tr>
<td>hello-interval</td>
<td>seconds</td>
</tr>
<tr>
<td>retrans-interval</td>
<td>seconds</td>
</tr>
<tr>
<td>transit-delay</td>
<td>seconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The **no** form of the command deletes the virtual link.
- It is possible to define areas in such a way that the backbone is no longer contiguous. In this case the system administrator can ensure backbone connectivity physically.
- Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.
- If authentication is enabled, both routers at either end of the virtual link must share the same password. Simple authentication refers to the use of only clear-text passwords as an authentication method. MD5 authentication refers to the usage of message digests.
- The **dead-interval** value should be the same for all routers on the same network. This value should be some multiple of the value given for the **hello interval**.

**Examples**

```bash
-> ip ospf virtual-link 0.0.0.1 172.22.2.115
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-key "techpubs"
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 auth-type simple
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 dead-interval 50
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 hello-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 retrans-interval 20
-> ip ospf virtual-link 0.0.0.1 172.22.2.115 transit-delay 50
-> no ip ospf virtual-link 0.0.0.1 172.22.2.115
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip ospf virtual-link` Displays the virtual link information.

**MIB Objects**

- `ospfVirtIfTable`
  - `ospfVirtIfAreaId`
  - `ospfVirtIfNeighbor`
  - `ospfVirtIfAuthKey`
  - `ospfVirtIfStatus`
  - `ospfVirtIfAuthType`
  - `ospfVirtIfRtrDeadInterval`
  - `ospfVirtIfHelloInterval`
  - `ospfVirtIfRetransInterval`
  - `ospfVirtIfTransitDelay`
ip ospf neighbor

Creates a static neighbor on a non-broadcast interface.

```
ip ospf neighbor neighbor_id {eligible | ineligible}
no ip ospf neighbor neighbor_id
```

### Syntax Definitions

- **neighbor_id**: A unique 32-bit IP address identical to the neighbor’s interface address.
- **eligible**: Sets this router as eligible to be the DR.
- **non-eligible**: Sets this router as not eligible to be the DR.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>eligible</td>
<td>ineligible</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- NBMA (Non Broadcast Multi Access), PMP (Point-to-Multipoint), and P2P (Point-to-Point) OSPF non-broadcast modes are supported over Ethernet interfaces (broadcast media).

- Neighboring routers on non-broadcast OSPF networks must be statically configured, because lack of OSPF multicast capabilities prevents using normal OSPF Hello protocol discovery.

- In the case of NBMA interface the static neighbor eligibility for becoming a DR can be configured while it is not necessary for point-to-multipoint and point-to-point interfaces.

- An interface connected to this neighbor must also be configured as a non-broadcast interface, which can be either point-to-multipoint or point-to-point, by using the `ip ospf interface type` command.

- For the correct working of an OSPF NBMA network, a fully meshed network is mandatory. Also, the neighbor eligibility configuration for a router on every other router should match the routers interface priority configuration.

### Examples

```
-> ip ospf neighbor 1.1.1.1 ineligible
-> no ip ospf neighbor 1.1.1.1
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip ospf interface type` Configures the OSPF interface type.
- `show ip ospf neighbor` Displays information on OSPF non-virtual neighbor routers.

**MIB Objects**

- `ospfNbrTable`
  - `ospfNbrPriority`
  - `ospfNbmaNbrStatus`
ip ospf redist-bgp-internal

Redistributes internal BGP routes (from the same AS) into OSPF protocol.

ip ospf redist-bgp-internal
no ip ospf redist-bgp-internal

Syntax Definitions
N/A

Defaults
By default, redistribution of iBGP routes is not allowed into OSPF protocol.

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples
-> ip ospf redist-bgp-internal
-> no ip ospf redist-bgp-internal

Release History
Release 8.7R2; command introduced.

Related Commands
show ip ospf
Displays the OSPF status and general configuration parameters.

MIB Objects
alaOspfRedistBgpInternal
ip ospf area

Assigns an OSPF interface to a specified area.

ip ospf area area_id [summary {enable | disable}] | [type {normal | stub | nssa}]

no ip ospf area area_id

Syntax Definitions

<table>
<thead>
<tr>
<th>area_id</th>
<th>A unique 32-bit value in IP address format.</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables summarization.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables summarization.</td>
</tr>
<tr>
<td>normal</td>
<td>Sets the area as a regular OSPF area. This parameter is not supported on an OmniSwitch 6560.</td>
</tr>
<tr>
<td>stub</td>
<td>Configures an OSPF area as a stub area.</td>
</tr>
<tr>
<td>nssa</td>
<td>Configures an OSPF area as a Not So Stubby Area (NSSA). This parameter is not supported on an OmniSwitch 6560.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>normal</td>
<td>stub</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The no form deletes the area.
- The summary options are used to enable or disable route summarization for stub and NSSA areas. Stub and NSSA areas will not receive LSA type 3 unless summary is enabled.
- The type command allows you to chose what type of area this is going to be.
- Consider the following when configuring an OSPF area ID on an OmniSwitch 6560:
  - Only one non-zero stub area is supported (configuring a 0.0.0.0 area ID is not allowed).
  - Only two IP OSPF interfaces can be associated with the area.
Examples
- `ip ospf area 0.0.0.1`
- `ip ospf area 0.0.0.1 type stub`
- `ip ospf area 0.0.0.1 type normal`
- `no ip ospf area 0.0.0.1`

Release History
Release 7.1.1; command was introduced.

Related Commands
- `ip ospf area default-metric` Creates or deletes an OSPF default metric.
- `ip ospf area range` Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
- `show ip ospf area` Displays either all OSPF areas, or a specified OSPF area.

MIB Objects
- `ospfAreaTable`
  - `ospfImportAsExtern`
  - `ospfAreaSummary`
  - `ospfAreaId`
ip ospf area default-metric

Creates or deletes a default metric for stub or Not So Stubby Area (NSSA) areas. The default metric configures the type of cost metric that a default area border router (ABR) will advertise in the default summary Link State Advertisement (LSA).

```
ip ospf area area_id default-metric tos [[cost cost] | [type {ospf | type 1 | type 2}]]
no ip ospf area area_id default-metric tos
```

**Syntax Definitions**

- `area_id` A unique 32-bit value in IP address format.
- `tos` Type of service. The valid range is 0–15. Only ToS value 0 is supported at this time.
- `cost` The numerical cost of this area and ToS. Only 0 is supported in the current release.
- `ospf` Advertises external routes as OSPF autonomous system external (ASE) routes.
- `type1` Advertises external routes as a Type 1 (non-OSPF) metric.
- `type2` Advertises external routes as a Type 2 (calculated weight value from non-OSPF protocol) metric.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>tos</td>
<td>0</td>
</tr>
<tr>
<td>ospf</td>
<td>type 1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The **no** form deletes the default metric from the specified area.
- The **type** command configures the type of cost metric for the specified ToS. To ensure that internal routers receiving external route advertisements choose the correct route, all border routers advertising a particular external network should be configured to advertise the route using the same metric type. That is, they must all advertise the route using an OSPF, Type 1, or Type 2 metric.
Examples

`-> ip ospf area 1.1.1.1 default-metric 0`
`-> no ip ospf area 1.1.1.1 default-metric 0`

Release History

Release 7.1.1; command was introduced.

Related Commands

- `ip ospf area` Creates or deletes an OSPF area.
- `ip ospf area range` Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
- `show ip ospf area` Displays either all OSPF areas, or a specified OSPF area.

MIB Objects

- `ospfStubAreaTable`
  - `ospfStubAreaId`
  - `ospfStubTOS`
  - `ospfStubStatus`
  - `ospfStubMetric`
  - `ospfStubMetricType`
**ip ospf area range**

Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

```
ip ospf area area_id range {summary | nssa} ip_address subnet_mask [effect {admatching | noMatching}] no ip ospf area area_id range {summary | nssa} ip_address subnet_mask
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area_id</td>
<td>A unique 32-bit value in IP address format.</td>
</tr>
<tr>
<td>summary</td>
<td>Advertises the address range as a summary link state advertisement (LSA).</td>
</tr>
<tr>
<td>nssa</td>
<td>Advertises the address range of Not So Stubby Area (NSSA) routes as a Type 5 advertisement. <em>This parameter is not supported on an OmniSwitch 6560.</em></td>
</tr>
<tr>
<td>ip_address</td>
<td>A 32-bit IP address for the range’s area.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>A 32-bit subnet mask that determines how many bits of the IP address denote the network number.</td>
</tr>
<tr>
<td>admatching</td>
<td>Determines that routes specified falling within the specified range will be advertised.</td>
</tr>
<tr>
<td>noMatching</td>
<td>Determines that any route falling within the specified range will not be advertised.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>nssa</td>
</tr>
<tr>
<td>admatching</td>
<td>noMatching</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Route summarization is the consolidation of addresses within an area which are advertised as a single route. When network numbers in an area are assigned consecutively, the area border router can be configured, using this command, to advertise a route that aggregates all the individual networks within the range.

- Using this command causes a single route to be advertised, for an address range in the specified area, to other areas.

- An NSSA (Not So Stubby Area) is similar to a stub area. However, where autonomous system (AS) external routes cannot be imported into a stub area, an NSSA will allow the importing of some AS external routes.

- Area ranges, once created, are enabled by default. Classless Inter-Domain Routing (CIDR) can work with OSPF to make route summarization more efficient. This is especially true for the summarization of routes in the global database. OSPF area address ranges can be configured on area border routers.

Examples

-> ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0
-> no ip ospf area 1.1.1.1 range summary 172.22.2.0 255.255.255.0

Release History

Release 7.1.1; command was introduced.

Related Commands

- **ip ospf area** Creates or deletes an OSPF area.
- **ip ospf area default-metric** Creates or deletes an OSPF default metric.
- **show ip ospf area range** Displays all or specified route summaries in a given area.

MIB Objects

- **ospfAreaAggregateTable**
- **ospfAreaAggregateAreaId**
- **ospfAreaAggregateLsdbType**
- **ospfAreaAggregateNet**
- **ospfAreaAggregateMask**
- **ospfAreaAggregateEffect**
- **ospfAreaAggregateStatus**
**ip ospf interface**

Creates and deletes an OSPF interface.

```
ip ospf interface {interface_name}
no ip ospf interface {interface_name}
```

**Syntax Definitions**

```
interface_name
```
The name of the interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to delete an OSPF interface.
- The interface name cannot contain spaces.

**Examples**

```
-> ip ospf interface vlan-101
-> no ip ospf interface vlan-101
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

**show ip ospf interface**

Displays the status and statistics of an OSPF interface.

**MIB Objects**

- `ospfIfTable`
  - `ospfIfIpAddress`
- `alaOspfIfAugTable`
- `alaOspfIfIntfName`
**ip ospf interface admin-state**

Enables or disables the administrative status on an OSPF interface.

```
ip ospf interface {interface_name} admin-state {enable | disable}
no ip ospf interface {interface_name} admin-state {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface_name</td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>64C2</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- Use the `no` form of the command to delete an OSPF interface.
- The OSPF interface must be enabled for it to participate in the OSPF protocol.

**Examples**

- `-> ip ospf interface vlan-101 admin-state enable`
- `-> ip ospf interface vlan-101 admin-state disable`
- `-> no ip ospf interface vlan-101 admin-state enable`
- `-> no ip ospf interface vlan-101 admin-state disable`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ip ospf interface*  
Displays the status and statistics of an OSPF interface.

**MIB Objects**

*ospfIfTable*

*ospfIfAdminStat*
**ip ospf interface area**

Configures an OSPF area identifier for this interface.

`ip ospf interface {interface_name} area area_id`

**Syntax Definitions**

- `interface_name`: The name of the interface.
- `area_id`: A unique 32-bit value in IP address format.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An interface must be assigned to an area to become operational.

**Examples**

```
-> ip ospf interface vlan-101 area 0.0.0.1
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip ospf area`: Displays either all the OSPF areas, or a specified OSPF area.
- `show ip ospf interface`: Displays the status and statistics of an OSPF interface.

**MIB Objects**

- `ospfIfTable`
- `ospfIfAreaId`
**ip ospf interface auth-key**

Configures an OSPF authentication key for simple authentication on an interface.

```
ip ospf interface {interface_name} auth-key key_string
```

### Syntax Definitions

- **interface_name**: The name of the interface.
- **key_string**: An authentication key (8 characters maximum).

### Defaults

The default for the authentication key string is a null string.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Sets a password as a simple text string of 8 ASCII characters.
- Must be used in conjunction with the **auth-type** command, described on page 27-37, set to **simple**.

### Examples

```
-> ip ospf interface vlan-101 auth-key pass
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **ip ospf interface auth-type**: Sets the authentication type.
- **show ip ospf interface**: Displays the status and statistics of an OSPF interface.

### MIB Objects

- ospfIfTable
  - ospfIfAuthKey
**ip ospf interface auth-type**

Sets the OSPF interface authentication type. Authentication allows the router to only respond to other routers that have the correct authentication information.

`ip ospf interface {interface_name} auth-type {none | simple | md5 | key-chain key-chain-id}`

---

**Syntax Definitions**

- **interface_name**: The name of the interface.
- **none**: No authentication.
- **simple**: Simple, clear text authentication.
- **md5**: MD5 encrypted authentication.
- **key-chain-id**: The configured key-chain ID.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>simple</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use this command to set the type of authentication that the OSPF interface uses to validate requests for route information from other OSPF neighbors on this interface.

- Simple authentication is authentication that uses only a text string as the password. The authentication type **simple** is used in conjunction with the **auth-key** keyword described, on page 27-36.

- MD5 authentication is encrypted authentication that uses an encryption key string and a key identification number. Both of these are necessary as the password. The authentication type **md5** is used in conjunction with the commands described on page 27-43 and page 27-45. One command enables MD5 and the other sets the key identification number.

- Use **keychain** to configure a keychain authentication type for an interface. When the OSPF interface receives a packet, the authentication information is carried in the hello packet. If the authentication succeeds, then adjacency is formed. The two remote machines must have the same active current key ID and same authentication type. Use **ip ospf interface auth-type none** to disassociate the keychain from the interface.
The authentication type can be set to SHA256 when using the `key-chain` parameter. The key ID and key must match between neighbors that are communicating with each other and must use a valid `start-time`. Refer to the `security key` and `security key-chain` commands for information on configuring the key-chain.

**Examples**

`-> ip ospf interface vlan-101 auth-type simple`

`-> ip ospf interface vlan-101 auth-type key-chain 1`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `key-chain` parameter added.

**Related Commands**

`ip ospf interface auth-key` Sets the password for simple authentication.

`show ip ospf interface` Displays the status and statistics of an OSPF interface.

`show ip ospf interface auth-info` Displays authentication information for the interface.

**MIB Objects**

`ospfIfTable`

`ospfIfAuthType`  
`alaOspfIfKeyChainId`
**ip ospf interface dead-interval**

Configures the OSPF interface dead interval.

```
ip ospf interface {interface_name} dead-interval seconds
```

**Syntax Definitions**

- `interface_name`: The name of the interface.
- `seconds`: The dead interval, in seconds. The valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>40 (broadcast and point-to-point)</td>
</tr>
<tr>
<td></td>
<td>120 (NBMA and point-to-multipoint)</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This is the interval, in seconds, after which a neighbor on this interface is considered dead if no hello packets have been received from this neighbor.
- This interval should be greater than the hello interval or the multiple of the hello interval.

**Examples**

```
-> ip ospf interface vlan-101 dead-interval 50
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- ip ospf interface hello-interval  Configures the OSPF interface hello interval.
- show ip ospf interface  Displays the status and statistics of an OSPF interface.

**MIB Objects**

ospfIfTable
  ospfIfRtrDeadInterval
ip ospf interface hello-interval

Configures the OSPF interface hello interval.

\texttt{ip ospf interface \{interface\_name\} hello-interval seconds}

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>10</td>
</tr>
<tr>
<td>(broadcast and point-to-point)</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
<tr>
<td>(NBMA and point-to-multipoint)</td>
<td></td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>10</td>
</tr>
<tr>
<td>(broadcast and point-to-point)</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
<tr>
<td>(NBMA and point-to-multipoint)</td>
<td></td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

This is the interval between two consecutive hello packets sent out on this interface.

### Examples

```
-> ip ospf interface vlan-101 hello-interval 50
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

show ip ospf interface
Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable

ospfIfHelloInterval
ip ospf interface md5

Creates and deletes the OSPF interface MD5 key identification number.

**ip ospf interface** *(interface_name)* md5 *key_id* [enable | disable]

### Syntax Definitions

- **interface_name**: The name of the interface.
- **key_id**: A key identification number. The key identification number specifies a number that allows MD5 encrypted routers to communicate. Both routers must use the same key ID. The valid range is 1–255.
- **enable**: Enables the interface key.
- **disable**: Disables the interface key.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- MD5 authentication can be used to encrypt information sent over the network. MD5 authentication works by using shared secret keys. Keys are used to sign the packets with an MD5 checksum, and they cannot be forged or tampered with. Since the keys are not included in the packet, snooping the key is not possible.
- This command is used in conjunction with the commands described on page 27-37 and page 27-45.
- The no variant deletes the key ID number.

### Examples

- `-> ip ospf interface vlan-101 md5 100`
- `-> ip ospf interface vlan-101 md5 10 disable`
- `-> ip ospf interface vlan-101 md5 10 enable`
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip ospf interface auth-type**  
  Sets the OSPF interface authentication type.
- **ip ospf interface md5 key**  
  Configures the OSPF key ID and key.
- **show ip ospf interface**  
  Displays the status and statistics of an OSPF interface.

**MIB Objects**

- **alaOspfIfMd5Table**
  - **alaOspfIfMd5IpAddress**
  - **alaOspfIfMd5KeyId**
ip ospf interface md5 key

Configures the OSPF key string. This interface MD5 string, along with the key identification number, enables the interface to encode MD5 encryption.

ip ospf interface {interface_name} md5 key_id key key_string

Syntax Definitions

interface_name The name of the interface.
key_id The key ID. The valid range is 1–255.
key_string A key string.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• This command is used in conjunction with the commands described above on page 27-37 and page 27-43.

• For MD5 authentication to function properly the same key string must be configured on the neighboring router for that interface.

Examples

-> ip ospf interface vlan-101 md5 100 key 1

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ip ospf interface auth-type`  Sets the OSPF interface authentication type.
- `ip ospf interface md5`  Creates and deletes the OSPF interface MD5 key identification number.
- `show ip ospf interface`  Displays the status and statistics of an OSPF interface.

**MIB Objects**

`alaOspfIfMd5Table`

- `alaOspfIfMd5IpAddress`
- `alaOspfIfMd5KeyId`
- `alaOspfIfMd5Key`
**ip ospf interface type**

Configures the OSPF interface type.

**ip ospf interface** `{interface_name}` type {point-to-point | point-to-multipoint | broadcast | non-broadcast}

---

**Syntax Definitions**

- **interface_name**
  - The name of the interface.
- **point-to-point**
  - Sets the interface to be a point-to-point OSPF interface.
- **point-to-multipoint**
  - Sets the interface to be a point-to-multipoint OSPF interface.
- **broadcast**
  - Sets the interface to be a broadcast OSPF interface.
- **non-broadcast**
  - Sets the interface to be NBMA (Non Broadcast Multi Access) OSPF interface.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>No</td>
</tr>
<tr>
<td>non-broadcast</td>
<td>No</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Yes</td>
</tr>
<tr>
<td>point-to-multipoint</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command sets an interface to be broadcast, non-broadcast, point-to-point, or point-to-multipoint.
- If the type is non-broadcast or point-to-multipoint, static neighbors should be configured.

---

**Examples**

- `-> ip ospf interface vlan-101 type non-broadcast`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ip ospf neighbor**  Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.

**show ip ospf interface**  Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfTable
ospfIfType
ip ospf interface cost

Configures the OSPF interface cost.

ip ospf interface {interface_name} cost cost

Syntax Definitions

interface_name  The name of the interface.
cost            The interface cost. The valid range is 0–65535.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost</td>
<td>1</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

The configured interface cost, if any, is used during OSPF route calculations.

Examples

-> ip ospf interface vlan-101 cost 10

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf interface  Displays the status and statistics of an OSPF interface.

MIB Objects

ospfIfMetricTable
  ospfIfMetricIpAddress
  ospfIfMetricValue
**ip ospf interface poll-interval**

Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.

```
ip ospf interface {interface_name} poll-interval seconds
```

### Syntax Definitions

- `interface_name` - The name of the interface.
- `seconds` - The poll interval, in seconds. The valid range is 1–2147483647.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>120</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This parameter configures the larger time interval, in seconds, between hello packets sent to an inactive neighbor.

### Examples

```
-> ip ospf interface vlan-101 poll-interval 500
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **show ip ospf interface** - Displays the status and statistics of an OSPF interface.

### MIB Objects

- `ospfIfTable` -
  - `ospfIfPollInterval`
**ip ospf interface priority**

Configures the OSPF interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

`ip ospf interface {interface_name} priority priority`

---

**Syntax Definitions**

- `interface_name`: The name of the interface.
- `priority`: The interface priority. The valid range is 0–255.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When two routers attached to a network both attempt to become the designated router, the one with the highest priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become the designated router.

**Examples**

`-> ip ospf interface vlan-101 priority 100`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ip ospf interface*  Displays the status and statistics of an OSPF interface.

**MIB Objects**

ospfIfTable
  
  ospfIfRtrPriority
**ip ospf interface retrans-interval**

Configures the OSPF interface retransmit interval.

```
ip ospf interface {interface_name} retrans-interval seconds
```

---

**Syntax Definitions**

- `interface_name` The name of the interface.
- `seconds` The retransmit interval, in seconds. The valid range 0–3600.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>5</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
```

---

**Usage Guidelines**

The number of seconds between link retransmission of OSPF packets on this interface.

---

**Examples**

```
-> ip ospf interface vlan-101 retrans-interval 500
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `show ip ospf interface` Displays the status and statistics of an OSPF interface.

---

**MIB Objects**

- `ospfIfTable`
- `ospfIfRetransInterval`
**ip ospf interface transit-delay**

Configures the OSPF interface transit delay.

```
ip ospf interface {interface_name} transit-delay seconds
```

### Syntax Definitions

- `interface_name`  
  The name of the interface.

- `seconds`  
  The transit delay, in seconds. The valid range is 0–3600.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The estimated number of seconds required to transmit a link state update over this interface. This command takes into account transmission and propagation delays and must be greater than 0.

### Examples

```
-> ip ospf interface vlan-101 transit-delay 100
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show ip ospf interface`  
  Displays the status and statistics of an OSPF interface.

### MIB Objects

- `ospfIfTable`  
  - `ospfIfTransitDelay`
ip ospf bfd-state

Enables or disables the registration of OSPF with the BFD protocol.

ip ospf bfd-state {enable | disable}

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables BFD for OSPF.</td>
<td>Disables BFD for OSPF.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- BFD must be globally enabled for the switch and OSPF must be registered with BFD at the protocol level before OSPF can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and the OSPF protocol acts based upon the BFD message.
- Whenever a neighbor goes down, OSPF will inform BFD to remove that neighbor from the BFD active list.

**Examples**

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of OSPF with the BFD protocol:

```
-> ip ospf bfd-state enable
-> ip ospf bfd-state disable
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip bfd admin-state**
  Enables or disables the global BFD protocol status for the switch.

- **ip ospf bfd-state all-interfaces**
  Enables or disables BFD for all OSPF interfaces configured.

- **ip ospf interface bfd-state**
  Enables or disables BFD for a specific OSPF interface.

- **ip ospf interface bfd-state drs-only**
  Establishes BFD sessions only on neighbors in full state.

- **ip ospf interface bfd-state all-neighbors**
  Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

- **show ip ospf**
  Displays OSPF status and general configuration parameters.

MIB Objects

- **alaProtocolospf**
- **alaOspfBfdStatus**
ip ospf bfd-state all-interfaces

Enables or disables BFD for all OSPF interfaces in the switch configuration.

ip ospf bfd-state all-interfaces {enable | disable}

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for all the OSPF interfaces.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for all the OSPF interfaces.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BFD status for OSPF must be enabled before OSPF can interact with BFD.

**Examples**

- `-> ip ospf bfd-state all-interfaces enable`
- `-> ip ospf bfd-state all-interfaces disable`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ip ospf bfd-state**  
  Enables or disables the BFD status for the OSPF protocol.

- **ip ospf interface bfd-state**  
  Enables or disables BFD for a specific OSPF interface.

- **ip ospf interface bfd-state drs-only**  
  Establishes BFD sessions only on neighbors in full state.

- **ip ospf interface bfd-state all-neighbors**  
  Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

- **show ip ospf interface**  
  Displays configuration information for an OSPF interface.

**MIB Objects**

- **alaProtocolospf**

  - **alaOspfBfdAllInterfaces**
ip ospf interface bfd-state

Enables or disables BFD for a specific OSPF interface.

**ip ospf interface if_name bfd-state {enable | disable}**

---

**Syntax Definitions**

- `if_name`: The name of an existing OSPF interface.
- `enable`: Enables BFD for the OSPF interface.
- `disable`: Disables BFD for the OSPF interface.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The BFD status for OSPF must be enabled before OSPF can interact with BFD.

---

**Examples**

-> ip ospf interface int1 bfd-state enable
-> ip ospf interface int2 bfd-state disable

---

**Release History**

Release 7.1.1; command was introduced.
OSPF Commands

ip ospf interface bfd-state

Enables or disables the BFD status for the OSPF protocol.

ip ospf bfd-state all-interfaces

Enables or disables BFD for all OSPF interfaces configured.

ip ospf interface bfd-state drs-only

Establishes BFD sessions only on neighbors in full state.

ip ospf interface bfd-state all-neighbors

Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

show ip ospf interface

Displays configuration information for an OSPF interface.

MIB Objects

alaOspfIfAugEntry

ospfIfIpAddress

alaOspfIfBfdStatus
**ip ospf interface bfd-state drs-only**

Establishes BFD sessions only with neighbors that are in the full state.

```
ip ospf interface if_name bfd-state drs-only
```

---

**Syntax Definitions**

`if_name` The name of an existing OSPF interface.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>drs-only</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

---

**Examples**

```
-> ip ospf interface int1 bfd-state drs-only
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip ospf bfd-state**
  Enables or disables the BFD status for OSPF protocol.

- **ip ospf bfd-state all-interfaces**
  Enables or disables BFD for all OSPF interfaces configured.

- **ip ospf interface bfd-state**
  Enables or disables BFD for a specific OSPF interface.

- **ip ospf interface bfd-state all-neighbors**
  Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

- **show ip ospf interface**
  Displays configuration information for an OSPF interface.

MIB Objects

- **alaOspfIfAugEntry**
  - **ospfIpIpAddress**
  - **alaOspfIfBfdDrsOnly**
ip ospf interface bfd-state all-neighbors

Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

ip ospf interface if_name bfd-state all-neighbors {enable | disable}

---

### Syntax Definitions

- **if_name**: The name of an existing OSPF interface.
- **enable**: Enables BFD sessions with all neighbors.
- **disable**: Disables BFD sessions with all neighbors.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/48C8/C32E/T24C2/</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The specified OSPF interface must be enabled to interact with BFD.
- The BFD status for OSPF must be enabled before OSPF can interact with BFD.

### Examples

- `-> ip ospf interface int1 bfd-state all-neighbors enable`
- `-> ip ospf interface int1 bfd-state all-neighbors disable`

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ip ospf bfd-state` Enables or disables the BFD status for OSPF protocol.
- `ip ospf bfd-state all-interfaces` Enables or disables BFD for all OSPF interfaces configured.
- `ip ospf interface bfd-state` Enables or disables BFD for a specific OSPF interface.
- `ip ospf interface bfd-state drs-only` Establishes BFD sessions only on neighbors in full state.
- `show ip ospf interface` Displays configuration information for an OSPF interface.

**MIB Objects**

- `alaOspfIfAugEntry`
  - `ospfIfIpAddress`
  - `alaOspfIfBfdDrsOnly`
**ip ospf restart-support**

Configures support for the graceful restart feature on an OSPF router.

```
ip ospf restart-support {planned-unplanned | planned-only}
no ip ospf restart-support
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>planned-unplanned</td>
<td>Specifies support for planned and unplanned restarts.</td>
</tr>
<tr>
<td>planned-only</td>
<td>This parameter is currently not supported.</td>
</tr>
</tbody>
</table>

**Defaults**

Graceful restart is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to disable support for the graceful restart feature on an OSPF router.
- The minimum hardware configuration for this command is a redundant CMM configuration.

**Examples**

```
-> ip ospf restart-support planned-unplanned
-> no ip ospf restart-support
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

```
show ip ospf restart
```

Displays the OSPF graceful restart related configuration and status.

**MIB Objects**

```
alaProtocolOspf
alaOspfRestartSupport
```
ip ospf restart-interval

Configures the grace period for achieving a graceful OSPF restart.

`ip ospf restart-interval [seconds]`

**Syntax Definitions**

*seconds* The hitless restart timeout interval. The valid range is 0–1800 seconds.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>120</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
No     No     Yes    No     Yes    Yes    Yes    Yes    Yes    Yes    Yes    Yes
```

**Usage Guidelines**

The minimum hardware configuration for this command is a redundant CMM configuration.

**Example**

```
-> ip ospf restart-interval 600
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip ospf restart-support` Administratively enables and disables support for the graceful restart feature on an OSPF router.
- `show ip ospf restart` Displays the OSPF graceful restart related configuration and status.

**MIB Objects**

alaProtocolOspf
    alaOspfRestartInterval
**ip ospf restart-helper admin-state**

Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.

**ip ospf restart-helper [admin-state {enable | disable}]**

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables the capability of an OSPF router to operate in helper mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the capability of an OSPF router to operate in helper mode.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The minimum hardware configuration for this command is a redundant CMM configuration.

**Examples**

-> ip ospf restart-helper admin-state disable
-> ip ospf restart-helper admin-state enable

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ip ospf restart-support**
  
  Administratively enables and disables support for the graceful restart feature on an OSPF router.

- **ip ospf restart-helper strict-lsa-checking admin-state**
  
  Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

- **show ip ospf restart**
  
  Displays the OSPF graceful restart related configuration and status.

**MIB Objects**

- `alaProtocolOspf`  
  - `alaOspfRestartHelperSupport`
**ip ospf restart-helper strict-lsa-checking admin-state**

Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

`ip ospf restart-helper strict-lsa-checking admin-state {enable | disable}`

---

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>enable</td>
</tr>
</tbody>
</table>

Enables whether or not a changed LSA will result in termination of graceful restart by a helping router.

Disables whether or not a changed LSA will result in termination of graceful restart by a helping router.

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>disable</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration.

---

### Examples

- `-> ip ospf restart-helper strict-lsa-checking admin-state disable`
- `-> ip ospf restart-helper strict-lsa-checking admin-state enable`

---

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **ip ospf restart-support**  
  Administratively enables and disables support for the graceful restart feature on an OSPF router.

- **ip ospf restart-helper admin-state**  
  Administratively enables and disables the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart.

- **show ip ospf restart**  
  Displays the OSPF graceful restart related configuration and status.

**MIB Objects**

- alaProtocolOspf  
- alaOspfRestartHelperSupport
**ip ospf restart initiate**

Initiates a planned graceful restart.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- You must execute this command on the primary CMM before executing a **takeover** command.
- The minimum hardware configuration for this command is a redundant CMM configuration.

**Example**

-> ip ospf restart initiate

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`show ip ospf restart` Displays the OSPF graceful restart related configuration and status.

**MIB Objects**

alaProtocolOspf
alaOspfRestartInitiate
**show ip ospf**

Displays the OSPF status and general configuration parameters.

```
show ip ospf
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is used to display the general configuration parameters of the OSPF router. See the Related Commands section below for commands that are used to modify the displayed parameters.

### Examples

```
-> show ip ospf
Router Id                        = 10.255.11.242,
OSPF Version Number              = 2,
Admin Status                     = Enabled,
Area Border Router ?             = No,
AS Border Router Status          = Enabled,
Route Tag                        = 0,
SPF Hold Time (in seconds)       = 10,
SPF Delay Time (in seconds)      = 5,
MTU Checking                     = Disabled,
# of Routes                      = 124,
# of AS-External LSAs            = 60,
# of self-originated LSAs        = 1,
# of LSAs received               = 118,
External LSDB Limit              = -1,
Exit Overflow Interval           = 0,
# of SPF calculations done        = 38395,
# of Incr SPF calculations done   = 0,
# of Init State Nbrs             = 0,
# of 2-Way State Nbrs            = 0,
# of Exchange State Nbrs         = 0,
# of Full State Nbrs             = 1,
```
# of attached areas = 1,
# of Active areas = 1,
# of Transit areas = 0,
# of attached NSSAs = 0,
Default Route Origination = none,
Default Route Metric-Type/Metric = type2 / 1,
BFD Status = Disabled
Opaque Transit Capability = Enabled
Redistribute internal BGP routes = Enabled

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Id</td>
<td>The unique identification for the router.</td>
</tr>
<tr>
<td>OSPF Version Number</td>
<td>The version of OSPF the router is running.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Whether OSPF is currently enabled or disabled on the router.</td>
</tr>
<tr>
<td>Area Border Router?</td>
<td>Whether the router status is an area router or not.</td>
</tr>
<tr>
<td>AS Border Router Status</td>
<td>Whether the area Autonomous System Border Router status of this router is enabled or disabled.</td>
</tr>
<tr>
<td>Route Tag</td>
<td>Shows the route tag for this router.</td>
</tr>
<tr>
<td>SPF Hold Time</td>
<td>Shows the time in seconds between the reception of an OSPF topology change and the start of a SPF calculation.</td>
</tr>
<tr>
<td>SPF Delay Time</td>
<td>Shows the time in seconds between consecutive SPF calculations.</td>
</tr>
<tr>
<td>MTU Checking</td>
<td>Shows whether Maximum Transfer Unit checking is enabled or disabled.</td>
</tr>
<tr>
<td># of Routes</td>
<td>The total number of OSPF routes known to this router.</td>
</tr>
<tr>
<td># of AS-External LSAs</td>
<td>The number of external routes learned from outside the router’s Autonomous System (AS).</td>
</tr>
<tr>
<td># of self-originated LSAs</td>
<td>The number of times a new Link State Advertisement has been sent from this router.</td>
</tr>
<tr>
<td># of LSAs received</td>
<td>The number of times a new Link State Advertisement has been received by this router.</td>
</tr>
<tr>
<td>External LSDB Limit</td>
<td>The maximum number of entries allowed in the external Link State Database.</td>
</tr>
<tr>
<td>Exit Overflow Interval</td>
<td>The number of seconds the router remains in the overflow state before attempting to leave it.</td>
</tr>
<tr>
<td># of SPF calculations done</td>
<td>The number of SPF calculations that have occurred.</td>
</tr>
<tr>
<td># of Incr SPF calculations done</td>
<td>The number of incremental SPF calculations done.</td>
</tr>
<tr>
<td># of Init State Nbrs</td>
<td>The number of neighbors in the initialization state.</td>
</tr>
<tr>
<td># of 2-Way State Nbrs</td>
<td>The number of OSPF 2-way state neighbors on this router.</td>
</tr>
<tr>
<td># of Exchange State Nbrs</td>
<td>The number of neighbors in the exchange state.</td>
</tr>
<tr>
<td># of Full State Nbrs</td>
<td>The number of neighbors in the full state.</td>
</tr>
<tr>
<td># of attached areas</td>
<td>The number of areas that are configured on the router.</td>
</tr>
<tr>
<td># of Active areas</td>
<td>The number of areas that are active.</td>
</tr>
<tr>
<td># of Transit areas</td>
<td>The number of transit areas that are configured on the router.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th># of attached NSSAs</th>
<th>The number of Not So Stubby Areas that are configured on the router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Route Origination</td>
<td>Whether route redistribution is enabled or disabled on the router.</td>
</tr>
<tr>
<td>Default Route Metric-Type/Metric</td>
<td>The default metric for stub or Not So Stubby Area (NSSA) areas. Specifies the type of cost metric that a default area border router (ABR) will advertise in the default summary Link State Advertisement (LSA).</td>
</tr>
<tr>
<td>BFD Status</td>
<td>Whether BFD monitoring is enabled or disabled for OSPF.</td>
</tr>
<tr>
<td>Opaque Transit Capability</td>
<td>Whether the opaque LSA accept and retransmit capability for OSPF is enabled or disabled.</td>
</tr>
<tr>
<td>Redistribute internal BGP routes</td>
<td>Whether redistribution of internal BGP routes into OSPF protocol is enabled or disabled.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.7R2; “Redistribute internal BGP routes” field added.

Related Commands

- `ip router router-id` Configures the router ID for the router.
- `ip ospf admin-state` Enables or disables the administration of OSPF on the router.
- `ip ospf route-tag` Configures a tag value for Autonomous System External (ASE) routes created.
- `ip ospf spf-timer` Configures timers for SPF calculation.
- `ip ospf mtu-checking` Enables or disables the use of Maximum Transfer Unit (MTU) checking.
- `ip ospf extlsdb-limit` Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.
- `ip ospf exit-overflow-interval` This command sets the overflow interval value.
- `ip ospf default-originate` Enables or disables OSPF redistribution
- `ip ospf area default-metric` Creates or deletes a default metric for stub or Not So Stubby Area (NSSA) areas.
- `ip ospf bfd-state` Enables or disables the registration of OSPF with the BFD protocol.
- `ip ospf redist-bgp-internal` This command allows redistribution of internal BGP routes into OSPF protocol.
**MIB Objects**

- ospfGeneralGroup
  - ospfRouterId
  - ospfAdminStat
  - ospfVersionNumber
  - ospfAreaBdrRtrStatus
  - ospfASBdrRtrStatus
  - ospfExternLsaCount
  - ospfExternLsaCksumSum
  - ospfTOSSupport
  - ospfOriginateNewLsas
  - ospfRxnNewLsas
  - ospfExtLsdbLimit
  - ospfExitOverflowInterval
  
- alaProtocolospf
  - alaOspfRedistRouteTag
  - alaOspfTimerSpfDelay
  - alaOspfTimerSpfHold
  - alaOspfRouteNumber
  - alaOspfMTUCheck
  - alaOspfOpaqueTransitCapability
  - alaOspfBfdStatus
**show ip ospf border-routers**

Displays information regarding all or specified border routers.

**show ip ospf border-routers [area_id] [router_id] [tos] [gateway]**

### Syntax Definitions

- **area_id**: A unique 32-bit value in IP address format.
- **router_id**: A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
- **tos**: The Type of Service. The valid range is 0–15. Only ToS value 0 is supported at this time.
- **gateway**: The 32-bit IP address of the gateway for the border router being displayed.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is used to display a list of border routers known by this OSPF router.
- By using the optional parameters, you can display the border routers using the specified parameter. For example, to find a router using a router ID of 1.1.1.1, enter the command using the router ID of 1.1.1.1 as a search criteria.
- See the related commands sections below to modify the list.

### Examples

```
-> show ip ospf border-routers 10.0.0.0

  Router Id | Area Id | Gateway | TOS | Metric
-------------+---------+---------+-----+--------
```

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 27-76
show ip ospf border-routers

<table>
<thead>
<tr>
<th>Router ID</th>
<th>10.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>1.0.0.1</td>
</tr>
<tr>
<td>Gateway</td>
<td>143.209.92.71</td>
</tr>
<tr>
<td>ToS</td>
<td>1</td>
</tr>
<tr>
<td>Metric</td>
<td>1</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The unique identification for the router.</td>
</tr>
<tr>
<td>Area ID</td>
<td>A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The next hop interface on which the border router has been learned.</td>
</tr>
<tr>
<td>ToS</td>
<td>The Type of Service. Only ToS value 0 is supported at this time.</td>
</tr>
<tr>
<td>Metric</td>
<td>The cost to the border router.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**show ip ospf**

Displays the OSPF status and general configuration parameters.

**MIB Objects**

alaOspfBdrRouterAreaId
alaOspfBdrRouterId
alaOspfBdrRouterTos
alaOspfBdrRouterMetric
**show ip ospf ext-lsdb**

Displays external Link State Advertisements known by this router.

```
show ip ospf ext-lsdb [linkstate-id ls_id] [router-id router_id]
```

### Syntax Definitions

- **ls_id**
  - The Link state ID. The ID is a unique 32-bit value such as an IP address. This number is used as a record in the link state database.

- **router_id**
  - The Router ID. The ID is a unique 32-bit value such as an IP address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is used to display the external link state database (LSDB) for the OSPF router.

- This command can be used for OSPF debugging purposes, specifically to narrow down sections of attached areas to determine which sections are receiving the specified external LSAs. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.

- See the Related Commands section below to modify the list.

### Examples

```
-> show ip ospf ext-lsdb

<table>
<thead>
<tr>
<th>LS Id</th>
<th>Orig Router-Id</th>
<th>SeqNo</th>
<th>Age</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>198.168.100.100</td>
<td>198.168.100.100</td>
<td>10</td>
<td>100</td>
<td>STATIC</td>
</tr>
</tbody>
</table>
```

### Output Definitions

- **LS Id**: The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.

- **Orig Router-Id**: The router ID of the router that originated the external LSDB.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeqNo</td>
<td>The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The type of protocol, if any.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**ip ospf extlsdb-limit** Assigns a limit to the number of External Link-State Database (LSDB) entries that can be learned.

**MIB Objects**

- ospfExtLsdbTable
  - ospfExtLsdbLsid
  - ospfExtLsdbRouterId
  - ospfExtLsdbSequence
  - ospfExtLsdbAge
  - ospfExtLsdbType
show ip ospf host

Displays information on the configured OSPF hosts.

show ip ospf host [ip_address]

Syntax Definitions

ip_address
A 32-bit IP address for a directly attached host.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is used to display general information for OSPF hosts directly attached to this router.
- See the Related Commands section below to modify the list.

Examples

-> show ip ospf host 172.22.2.115

<table>
<thead>
<tr>
<th>Host Address</th>
<th>TOS</th>
<th>Metric</th>
<th>Status</th>
<th>AreaId</th>
</tr>
</thead>
<tbody>
<tr>
<td>143.209.92.12</td>
<td>1</td>
<td>0</td>
<td>Up</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Host Address</th>
<th>A 32-bit IP address for a directly attached host. This can be set using the ip ospf host command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ToS</td>
<td>The Type of Service traffic from the host is labeled as. ToS is set using the ip ospf host command.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric assigned to the host. Metric is set using the ip ospf host command.</td>
</tr>
<tr>
<td>Status</td>
<td>Whether the host is enabled or disabled.</td>
</tr>
<tr>
<td>AreaId</td>
<td>The area identification for the host’s area.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

*ip ospf host*  
Creates and deletes an OSPF entry for directly attached hosts.

**MIB Objects**

* ospfHostTable  
  * ospfHostIpAddress  
  * ospfHostTOS  
  * ospfHostMetric  
  * ospfHostStatus  
  * ospfHostAreaID
**show ip ospf lsdb**

Displays LSAs in the Link State Database associated with each area.

```
show ip ospf lsdb [area_id] [rtr | net | netsum | asbrsum] [linkstate-id ls_id] [router-id router_id]
```

### Syntax Definitions

- **area_id**: A unique 32-bit value in IP address format.
- **rtr**: Specifies router LSAs.
- **net**: Specifies network LSAs.
- **netsum**: Specifies network summary LSAs.
- **asbrsum**: Specifies Autonomous System Border Router summary LSAs.
- **ls_id**: The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
- **router_id**: The Router ID. The ID is a unique 32-bit value such as an IP address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860M</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is used to display the Link State Database (LSDB) of the OSPF router. This command can be used for OSPF debugging purposes, specifically to narrow down sections of an area to determine which sections are receiving the specified link state advertisements. You may specify only the parameters from the area LSDB in which you are interested using the optional command parameters.

- You can view link state advertisements by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you must also supply a valid link state ID.

### Examples

```
-> show ip ospf lsdb
Area Id  Type  LS Id        Orig Router-Id  SeqNo  Age
--------------------------------------------------------
0.0.0.1  OSPF  198.168.100.100  198.168.100.100  1    100
```
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Id</td>
<td>The area identification for the area to which the record belongs.</td>
</tr>
<tr>
<td>Type</td>
<td>The protocol type from where the route was learned.</td>
</tr>
<tr>
<td>LS Id</td>
<td>The Link state ID. The ID is a unique 32-bit value such as an IP address.</td>
</tr>
<tr>
<td>Orig Router-Id</td>
<td>The router ID of the router that originated the external LSDB.</td>
</tr>
<tr>
<td>SeqNo</td>
<td>The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip ospf

Displays the OSPF status and general configuration parameters.

MIB Objects

ospfLsdbTable
  ospfLsdbAreaId
  ospfLsdbType
  ospfLsdbLsid
  ospfLsdbRouterId
  ospfLsdbSequence
  ospfLsdbAge


**show ip ospf neighbor**

Displays information on OSPF non-virtual neighbor routers.

`show ip ospf neighbor [ip_address]`

---

**Syntax Definitions**

`ip_address` A 32-bit IP address of the neighboring router.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command is used to display all non-virtual neighbors of the OSPF router.
- See the Related Commands section below to modify the list.

---

**Examples**

```
-> show ip ospf neighbor

            IP Address  Area Id  Router Id  Domain Name  Domain ID  State  Type
-------------------------------------------+----------------------+
            12.1.1.2      0.0.0.1  2.2.2.2   Vlan         12     Full   Dynamic
            10.1.1.1      0.0.0.0  1.1.1.1   Tunnel       NA     Full   Dynamic
            13.1.1.2      0.0.0.1  3.3.3.3   Service      1200   Full   Dynamic
```

---

**output definitions**

- **IP Address** The IP address of the neighbor.
- **Area Id** A unique 32-bit value, such as an IP address, that identifies the neighboring router in the Autonomous System.
- **Router Id** The unique identification for the neighboring router.
- **Domain Name** The domain on which the neighbor is reachable (VLAN, Service, or Tunnel).
- **Domain ID** The VLAN ID or service ID on which the neighbor is reachable. This field displays “NA” for IP tunnels.
### show ip ospf neighbor

| Neighbor's IP Address | Neighbor's Router Id | Neighbor's Area Id | Neighbors's Domain Name | Neighbors's Domain ID | Neighbor's DR Address | Neighbor's BDR Address | Neighbor's Priority/Eligibility | Neighbor's State | Hello Suppressed? | Neighbor's type | # of State Events | Mode | MD5 Sequence Number | Time since Last Hello | # of Outstanding LS Requests | # of Outstanding LS Acknowledgements | # of Outstanding LS Retransmissions | Restart Helper Status | Restart Age (in seconds) | Last Restart Helper Exit Reason | Opaque LSA Capability |
|-----------------------|----------------------|-------------------|-------------------------|-----------------------|-----------------------|------------------------|---------------------------|-----------------|----------------|----------------|-----------------|------|---------------------|--------------------------|-----------------------------|-----------------------------|------------------------|------------------------|----------------------|------------------------|
| 12.1.1.2              | 2.2.2.2              | 0.0.0.1           | Vlan                    | 0.0.0.1               | 12.1.1.2              | 12.1.1.1              | 1                         | Full            | No             | Dynamic       | 6                | Slave | 0                   | 7 sec                    | 0                           | 0                           | notHelping             | 0 sec                  | None                 | Yes                    |
| 14.1.1.2              | 3.3.3.3              | 0.0.0.1           | Service                 | 1200                  | 13.1.1.2              | 13.1.1.1              | 1                         | Full            | No             | Dynamic       | 6                | Slave | 0                   | 7 sec                    | 0                           | 0                           | notHelping             | 0 sec                  | None                 | Yes                    |
| 10.1.1.1              | 1.1.1.1              | 0.0.0.0           | Tunnel                  |                       |                       |                       |                           |                 |               |               |                 |       |                     |                          |                             |                             |                        |                       |                      |                       |

**output definitions (continued)**

**State**
The state of the OSPF neighbor adjacency.

**Type**
What type of neighbor, either Dynamic (learned) or Static.
Neighbors's Domain ID = NA,
Neighbor's DR Address = 10.1.1.1,
Neighbor's BDR Address = 0.0.0.0,
Neighbor's Priority/Eligibility = 1,
Neighbor's State = Full,
Hello Suppressed ? = No,
Neighbor's type = Dynamic,
# of State Events = 6,
Mode = Master,
MD5 Sequence Number = 0,
Time since Last Hello = 7 sec,
# of Outstanding LS Requests = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions = 0,
Restart Helper Status = notHelping,
Restart Age (in seconds) = 0 sec,
Last Restart Helper Exit Reason = None
Opaque LSA Capability = Yes

output definitions

<table>
<thead>
<tr>
<th>Neighbor’s IP Address</th>
<th>The IP address of the neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor’s Router Id</td>
<td>The identification number for the selected host’s record. It is most often the router’s IP address.</td>
</tr>
<tr>
<td>Neighbor’s Area Id</td>
<td>Identifier of the OSPF Area to which the neighbor is attached. 255.255.255.255 shows that this neighbor is not attached to any area.</td>
</tr>
<tr>
<td>Neighbor’s Domain Name</td>
<td>The domain on which the neighbor is reachable (VLAN, Service, or Tunnel).</td>
</tr>
<tr>
<td>Neighbor’s Domain ID</td>
<td>The VLAN ID or service ID on which the neighbor is reachable. This field displays “NA” for IP tunnels.</td>
</tr>
<tr>
<td>Neighbor's DR Address</td>
<td>The address of the neighbors Designated Router.</td>
</tr>
<tr>
<td>Neighbor's BDR Address</td>
<td>The address of the neighbors Backup Designated Router.</td>
</tr>
<tr>
<td>Neighbor's Priority</td>
<td>The priority value for this neighbor becoming the DR.</td>
</tr>
<tr>
<td>Neighbor's State</td>
<td>The condition of the OSPF neighbor’s state machine.</td>
</tr>
<tr>
<td>Hello Suppressed</td>
<td>Whether sending hello messages to this neighbor is suppressed.</td>
</tr>
<tr>
<td>Neighbor’s type</td>
<td>What type of neighbor this is, either dynamic or static.</td>
</tr>
<tr>
<td>DR Eligible</td>
<td>Shows the eligibility status of the static neighbor. If it is configured as “ineligible” during creation of the neighbor, it shows up as No. Otherwise, if configured as Eligible (the default), it shows up as Yes.</td>
</tr>
<tr>
<td># of State Events</td>
<td>The number of state events restricted for this neighbor and the local router.</td>
</tr>
<tr>
<td>Mode</td>
<td>The role the neighbor has with the local router during DD Exchange, which can be Master or Slave.</td>
</tr>
<tr>
<td>MD5 Sequence Number</td>
<td>The sequence number of the MD5 authorization key.</td>
</tr>
<tr>
<td>Time since Last Hello</td>
<td>The amount of time (in seconds) since the last HELLO messages was received from this neighbor.</td>
</tr>
<tr>
<td># of Outstanding LS Requests</td>
<td>The number of Link State requests to this neighbor that have not received a response from this neighbor.</td>
</tr>
</tbody>
</table>
Release History

Release 7.1.1; command was introduced.
Release 8.6R1; “Domain Name”, “Domain ID”, “Neighbor’s Domain Name”, and “Neighbor’s Domain ID” fields added.

Related Commands

ip ospf neighbor

Creates a static neighbor on a Non Broadcast Multi Access (NBMA) interface.

MIB Objects

ospfNbrTable
  ospfNbrIpAddr
  ospfNbrRtrId
  ospfNbrOptions
  ospfNbrPriority
  ospfNbrState
  ospfNbrEvents
  ospfNbrHelloSuppressed
alaOspfNbrAugTable
  alaOspfNbrRestartHelperStatus
  alaOspfNbrRestartHelperAge
  alaOspfNbrRestartHelperExitReason
  alaOspfNbrAreaId
  alaOspfNbrDrAddress
  alaOspfNbrBdrAddress
  alaOspfNbrType
  alaOspfNbrMode
  alaOspfNbrMd5SeqNo
  alaOspfNbrLastHello
  alaOspfNbrPendingLSreq
  alaOspfNbrPendingLSack
  alaOspfNbrPendingLSupd
  alaOspfNbrIfIndex

output definitions (continued)

<table>
<thead>
<tr>
<th># of Outstanding LS Acknowledgements</th>
<th>Number of Link state Acknowledgements queued up by the local router to be sent to the neighbor.</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Outstanding LS Retransmissions</td>
<td>The number of Link State updates to the neighbor that need to be retransmitted by the OSPF router.</td>
</tr>
<tr>
<td>Restart Helper Status</td>
<td>Indicates whether the router is acting as a hitless restart helper for the neighbor.</td>
</tr>
<tr>
<td>Restart Age</td>
<td>The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the neighbor.</td>
</tr>
<tr>
<td>Last Restart Helper Exit Reason</td>
<td>The outcome of the last attempt at acting as a hitless restart helper for the neighbor.</td>
</tr>
<tr>
<td>Opaque LSA Capability</td>
<td>Whether the opaque LSA accept and retransmit capability for OSPF is enabled or disabled.</td>
</tr>
</tbody>
</table>
**show ip ospf routes**

Displays the OSPF routes known to the router.

`show ip ospf routes [ip_address mask tos gateway]`

---

**Syntax Definitions**

- **ip_address**: A 32-bit IP address of the route destination in dotted decimal format.
- **mask**: The IP subnet mask of the route destination.
- **tos**: The Type of Service of the route.
- **gateway**: The next hop IP address for this router.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no variables are entered, all routes are displayed. If the variables are entered, then only routes matching the specified criteria are shown. All the variables described above must be entered for a route match. If all of the variables are not entered, an error message is returned.

**Examples**

```
-> show ip ospf routes
```

<table>
<thead>
<tr>
<th>Destination/Mask</th>
<th>Gateway</th>
<th>Metric</th>
<th>Domain Name</th>
<th>Domain ID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.2/32</td>
<td>12.1.1.2</td>
<td>1</td>
<td>Vlan</td>
<td>12</td>
<td>Intra</td>
</tr>
<tr>
<td>12.1.1.0/24</td>
<td>12.1.1.1</td>
<td>1</td>
<td>Vlan</td>
<td>12</td>
<td>Intra</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>10.1.1.2</td>
<td>1</td>
<td>Tunnel</td>
<td>NA</td>
<td>Intra</td>
</tr>
<tr>
<td>20.1.1.0/24</td>
<td>120.1.1.2</td>
<td>2</td>
<td>Service</td>
<td>120</td>
<td>Inter</td>
</tr>
<tr>
<td>172.28.4.0/24</td>
<td>120.1.1.2</td>
<td>2</td>
<td>Service</td>
<td>120</td>
<td>Inter</td>
</tr>
<tr>
<td>198.168.100.100</td>
<td>195.5.2.8</td>
<td>0</td>
<td>Vlan</td>
<td>5</td>
<td>AS-Ext</td>
</tr>
</tbody>
</table>

**output definitions**

- **Destination/Mask**: The destination address of the route. This can also display the destination IP address mask if it is known.
- **Gateway**: The gateway address of the route.
**output definitions**

<table>
<thead>
<tr>
<th>Metric</th>
<th>The cost of the route.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>The domain on which the gateway can be routed (VLAN, Service, or Tunnel).</td>
</tr>
<tr>
<td>Domain ID</td>
<td>The VLAN ID or service ID on which the gateway can be routed. This field displays “NA” for IP tunnels.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of OSPF route.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.6R2; “Domain Name” and “Domain ID” fields added.

**Related Commands**

- **show ip ospf**  
  Displays the OSPF status and general configuration parameters.

**MIB Objects**

- alaOspfRouteTable
  - alaOspfRouteDest
  - alaOspfRouteMask
  - alaOspfRouteNextHop
  - alaOspfRouteIfIndex
  - alaOspfRouteType
  - alaOspfRouteMetric1
**show ip ospf virtual-link**

Displays virtual link information. A virtual link is used to connect OSPF backbone routers that are not physically contiguous.

**show ip ospf virtual-link [router_id]**

---

### Syntax Definitions

`router_id`  
The router ID of the remote end of the virtual link that is to be viewed.

---

### Defaults

N/A

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

See the Related Commands section below to modify the list.

---

### Examples

```bash
-> show ip ospf virtual-link
```

<table>
<thead>
<tr>
<th>Transit AreaId</th>
<th>Router-id</th>
<th>Link / Adjacency</th>
<th>AuthType</th>
<th>OperStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>172.17.1.1</td>
<td>P2P / Full</td>
<td>none</td>
<td>up</td>
</tr>
</tbody>
</table>

---

### Output definitions

- **Transit AreaId**: The area identification for the area assigned to the virtual link.
- **Router-Id**: The destination router identification for the virtual link.
- **State Link**: The state of the virtual link with regards to the local router.
- **State Adjacency**: The state of the virtual link adjacency.
- **AuthType**: The type of authorization employed by the virtual link.
- **OperStatus**: Displays whether the virtual link is enabled or disabled.

---

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip ospf virtual-link** Creates or deletes a virtual link.
- **show ip ospf virtual-neighbor** Displays OSPF virtual neighbors.

MIB Objects

- **ospfVirtIfTable**
  - **ospfVirtIfAreaId**
  - **ospfVirtIfNeighbor**
  - **ospfVirtIfState**
  - **ospfVirtIfAuthType**
show ip ospf virtual-neighbor

Displays OSPF virtual neighbors. A virtual neighbor is connected to the router through a virtual link rather than a physical one.

show ip ospf virtual-neighbor area_id router_id

Syntax Definitions

area_id
A unique 32-bit value in IP address format.

router_id
The router ID of the remote end of the virtual link that is to be viewed.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is used to display all virtual neighbors for the OSPF router.
- See the Related Commands section below to modify the list.

Examples

-> show ip ospf virtual-neighbor 0.0.0.0 10.0.0.1

<table>
<thead>
<tr>
<th>AreaId</th>
<th>RouterId</th>
<th>Priority</th>
<th>Events</th>
<th>RxmtQlen</th>
<th>LastHello</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>10.0.0.0</td>
<td>1</td>
<td>10</td>
<td>100</td>
<td>323</td>
<td>INIT</td>
</tr>
</tbody>
</table>

output definitions

AreaId
The area identification for the area of which the virtual neighbor is a part.

RouterId
The router identification of the virtual neighbor.

Priority
The number used to determine whether the virtual neighbor will become the designated router for its area.

Events
The number of OSPF control message sent by the neighbor to the router.

RxmtQlen
The length (in number of packets) of the retransmit queue.
-> show ip ospf virtual-neighbor 0.0.0.1 2.0.0.254
Neighbor's IP Address    = 2.0.0.254,
Neighbor's Router Id    = 2.0.0.254,
Neighbor's Area Id      = 0.0.0.1,
Neighbor's DR Address   = 2.0.0.1,
Neighbor's BDR Address  = 2.0.0.254,
Neighbor's Priority     = 1,
Neighbor's State        = Full,
Hello Suppressed ?      = No,
Neighbor's type         = Dynamic,
# of State Events       = 6,
Mode                    = Master,
MD5 Sequence Number     = 0,
Time since Last Hello   = 5 sec,
Last DD I_M_MS          =
# of Outstanding LS Requests = 0,
# of Outstanding LS Acknowledgements = 0,
# of Outstanding LS Retransmissions = 0,
Restart Helper Status   = Not Restarting,
Restart Age (in seconds) = 0 sec,
Last Restart Helper Exit Reason = None

output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastHello</td>
<td>The last Hello message sent by the neighbor</td>
</tr>
<tr>
<td>State</td>
<td>The current state the virtual neighbor is in relative to the router; this</td>
</tr>
<tr>
<td></td>
<td>will be INIT, Exchange, or Full.</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor’s IP Address</td>
<td>The IP address of the virtual neighbor.</td>
</tr>
<tr>
<td>Neighbor’s Router Id</td>
<td>The identification number for the selected host’s record. It is most often</td>
</tr>
<tr>
<td></td>
<td>the router’s IP address.</td>
</tr>
<tr>
<td>Neighbor’s Area Id</td>
<td>Identifier of the OSPF Area to which the virtual neighbor is attached.</td>
</tr>
<tr>
<td></td>
<td>255.255.255.255 shows that this virtual neighbor is not attached to any</td>
</tr>
<tr>
<td></td>
<td>area.</td>
</tr>
<tr>
<td>Neighbor’s DR Address</td>
<td>The address of the virtual neighbor’s Designated Router.</td>
</tr>
<tr>
<td>Neighbor’s BDR Address</td>
<td>The address of the virtual neighbor’s Backup Designated Router.</td>
</tr>
<tr>
<td>Neighbor’s Priority</td>
<td>The priority value for this virtual neighbor becoming the DR.</td>
</tr>
<tr>
<td>Neighbor's State</td>
<td>The condition of the OSPF virtual neighbor’s state machine.</td>
</tr>
<tr>
<td>Hello Suppressed</td>
<td>Whether sending hello messages to this virtual neighbor is suppressed.</td>
</tr>
<tr>
<td>Neighbor’s type</td>
<td>What type of virtual neighbor this is, either dynamic or static.</td>
</tr>
<tr>
<td>DR Eligible</td>
<td>Shows the eligibility status of the virtual neighbor. If it is configured</td>
</tr>
<tr>
<td></td>
<td>as “ineligible” during creation of the neighbor, it shows up as No.</td>
</tr>
<tr>
<td></td>
<td>Otherwise, if configured as Eligible (the default), it shows up as Yes.</td>
</tr>
<tr>
<td># of State Events</td>
<td>The number of state events restricted for this virtual neighbor and the</td>
</tr>
<tr>
<td></td>
<td>local router.</td>
</tr>
<tr>
<td>Mode</td>
<td>The role the virtual neighbor has with the local router during DD Exchange,</td>
</tr>
<tr>
<td></td>
<td>which can be Master or Slave.</td>
</tr>
<tr>
<td>MD5 Sequence Number</td>
<td>The sequence number of the MD5 authorization key.</td>
</tr>
</tbody>
</table>
### Output Definitions (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time since Last Hello</strong></td>
<td>The amount of time (in seconds) since the last HELLO messages was received from this virtual neighbor.</td>
</tr>
<tr>
<td><strong>Last DD I_M_MS</strong></td>
<td>The initialize (I), more (M) and master (MS) bits, and Options field Data Description (DD) packet received from the virtual neighbor. This parameter is used to determine whether the next DD packet has been received or not.</td>
</tr>
<tr>
<td><strong># of Outstanding LS Requests</strong></td>
<td>The number of Link State requests to this virtual neighbor that have not received a response from this virtual neighbor.</td>
</tr>
<tr>
<td><strong># of Outstanding LS Acknowledgements</strong></td>
<td>Number of Link State Acknowledgements queued up by the local router to be sent to the virtual neighbor.</td>
</tr>
<tr>
<td><strong># of Outstanding LS Retransmissions</strong></td>
<td>The number of Link State updates to the virtual neighbor that need to be retransmitted by the OSPF router.</td>
</tr>
<tr>
<td><strong>Restart Helper Status</strong></td>
<td>Indicates whether the router is acting as a hitless restart helper for the virtual neighbor.</td>
</tr>
<tr>
<td><strong>Restart Age</strong></td>
<td>The remaining time, in seconds, for the current OSPF hitless restart interval if the router is acting as a restart helper for the virtual neighbor.</td>
</tr>
<tr>
<td><strong>Last Restart Helper Exit Reason</strong></td>
<td>The outcome of the last attempt at acting as a hitless restart helper for the virtual neighbor.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command was introduced.

### Related Commands

**ip ospf virtual-link**  
Creates or deletes a virtual link.

### MIB Objects

- `ospfVirtNbrTable`
  - `ospfVirtNbrArea`
  - `ospfVirtNbrRtrId`
  - `ospfVirtNbrState`
- `alaOspfVirtNbrAugTable`
  - `alaOspfVirtNbrRestartHelperStatus`
  - `alaOspfVirtNbrRestartHelperAge`
  - `alaOspfVirtNbrRestartHelperExitReason`
show ip ospf area

Displays either all OSPF areas, or a specified OSPF area.

show ip ospf area [area_id]

Syntax Definitions

area_id A unique 32-bit value in IP address format.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Allows you to view the details of a specified OSPF area.
- Not specifying an OSPF area will display all known areas for the OSPF router.
- See the Related Commands section below for information on modifying an area.

Examples

-> show ip ospf area

<table>
<thead>
<tr>
<th>Area Id</th>
<th>AdminStatus</th>
<th>Type</th>
<th>OperStatus</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>disabled</td>
<td>normal</td>
<td>down</td>
</tr>
<tr>
<td>0.0.0.1</td>
<td>disabled</td>
<td>normal</td>
<td>down</td>
</tr>
</tbody>
</table>

-> show ip ospf area 0.0.0.0

Area Identifier = 1.1.1.1,
Admin Status = Disabled,
Operational Status = Down,
Area Type = Enabled,
Area Summary = Enabled,
Time since last SPF Run = 00h:00m:27s,
# of Area Border Routers known = 0,
# of AS Border Routers known = 0,
# of LSAs in area = 0,
# of SPF Calculations done = 0,
# of Incremental SPF Calculations done = 0,
# of Neighbors in Init State = 0,
# of Neighbors in 2-Way State = 0,
# of Neighbors in Exchange State = 0,
# of Neighbors in Full State = 0,
# of Interfaces attached = 0
Attached Interfaces = vlan-213

output definitions

<table>
<thead>
<tr>
<th>Area Identifier</th>
<th>The unique 32-bit value, such as IP address, that identifies the OSPF area in the AS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Status</td>
<td>Whether the area is enabled or disabled.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Whether the area is active.</td>
</tr>
<tr>
<td>Area Type</td>
<td>The area type. This field will be normal, stub, or NSSA.</td>
</tr>
<tr>
<td>Area Summary</td>
<td>Whether Area Summary is enabled or disabled.</td>
</tr>
<tr>
<td>Time since last SPF Run</td>
<td>The last time the Shortest Path First calculation was performed.</td>
</tr>
<tr>
<td># of Area Border Routers known</td>
<td>The number of Area Border Routers in the area.</td>
</tr>
<tr>
<td># of AS Border Routers known</td>
<td>The number of Autonomous System Border Routers in the area.</td>
</tr>
<tr>
<td># of LSAs</td>
<td>The total number of Link State Advertisements for the Area.</td>
</tr>
<tr>
<td># of SPF Calculations</td>
<td>The number of times the area has calculated the Shortest Path.</td>
</tr>
<tr>
<td># of Incremental SPF Calculations</td>
<td>The number of incremental Shortest Path First calculations that have been performed in the area.</td>
</tr>
<tr>
<td># of Neighbors in Init State</td>
<td>The number of OSPF neighbors that are in initialization.</td>
</tr>
<tr>
<td># of Neighbors in 2-Way State</td>
<td>The number of OSPF 2-way state neighbors in this area.</td>
</tr>
<tr>
<td># of Neighbors in Exchange State</td>
<td>The number of OSPF neighbors that are currently establishing their status.</td>
</tr>
<tr>
<td># of Neighbors in Full State</td>
<td>The number of OSPF neighbors.</td>
</tr>
<tr>
<td># of Interfaces attached</td>
<td>The number of OSPF interfaces.</td>
</tr>
<tr>
<td>Attached Interfaces</td>
<td>The names of the OSPF interfaces attached to this area.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

*ip ospf area* Creates or deletes an OSPF area, assigning default metric, cost, and type.
*ip ospf area range* Creates a route summarization instance whereby a range of addresses will be advertised as a single route.
*show ip ospf interface* Displays OSPF interface information.
**MIB Objects**

`ospfAreaTable`  
  - `ospfAreaId`  
  - `ospfImportAsExtern`  
  - `ospfSpfRuns`  
  - `ospfAreaBdrRtrCount`  
  - `ospfAsBdrRtrCount`  
  - `ospfAreaLsaCount`  
  - `ospfAreaSummary`  
  - `ospfAreaStatus`  

`alaOspfIfAugTable`  
  - `alaOspfIfIntfName`
show ip ospf area range

Displays all or specified route summaries in a given area.

**show ip ospf area area_id range [summary | nssa] ip_address ip_mask**

**Syntax Definitions**

- **area_id**: A unique 32-bit value in IP address format.
- **summary**: Specifies that routes are summarized.
- **nssa**: Specifies the Not So Stubby Area (NSSA) routers are summarized. *This parameter is not supported on an OmniSwitch 6560.*
- **ip_address**: A 32-bit IP address.
- **ip_mask**: A 32-bit subnet mask.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Allows you to view the details of a specified OSPF area range.
- See the Related Commands section below for information on modifying an area.

**Examples**

-> show ip ospf area 0.0.0.0 range

<table>
<thead>
<tr>
<th>AreaId</th>
<th>Type</th>
<th>Destination</th>
<th>Advertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Summary</td>
<td>192.168.12.1/24</td>
<td>Matching</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>NSSA</td>
<td>143.209.92.71/24</td>
<td>noMatching</td>
</tr>
</tbody>
</table>

**output definitions**

- **AreaId**: The area identification for the area range.
- **Type**: The type of area the range is associated with.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
<td>The destination address of the range.</td>
</tr>
<tr>
<td><strong>Advertise</strong></td>
<td>Shows the filter effect of the range. LSAs in the range are either advertised (Matching) or not advertised (noMatching).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**ip ospf area range**

Creates a route summarization instance whereby a range of addresses assigned for the route at the area border router will be advertised.

**MIB Objects**

ospfAreaRangeTable
- ospfAreaRangeAreaId
- ospfAreaRangeNet
- ospfAreaRangeMask
- ospfAreaRangeStatus
- ospfAreaRangeEffect
**show ip ospf area stub**

Displays stub default area metrics, if configured.

**show ip ospf area area_id stub**

---

**Syntax Definitions**

`area_id`  
A unique 32-bit value in IP address format.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> show ip ospf area 0.0.0.1 stub`

<table>
<thead>
<tr>
<th>Area Id</th>
<th>TOS</th>
<th>Metric</th>
<th>MetricType</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.1</td>
<td>1</td>
<td>1</td>
<td>ospf</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Area Id</th>
<th>The identification number of the stub area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>TOS</td>
<td>The Type of Service assignment.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric assignment of the default router in the stub area.</td>
</tr>
<tr>
<td>MetricType</td>
<td>The metric type of the stub area. It will be either ospf, type1, or type2.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ip ospf area**
Creates or deletes an OSPF area.

MIB Objects

ospfStubAreaTable
  ospfStubAreaId
  ospfStubTOS
  ospfStubMetric
  ospfStubStatus
  ospfStubMetricType
**show ip ospf interface**

Displays OSPF interface information.

*show ip ospf interface [interface_name]*

---

**Syntax Definitions**

interface_name The name of the interface.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Not specifying an interface name displays all known interfaces for the OSPF router.

---

**Examples**

No interface name is specified:

```
-> show ip ospf interface
```

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>DR Address</th>
<th>Backup DR Address</th>
<th>Admin Status</th>
<th>Oper Status</th>
<th>BFD Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-213</td>
<td>100.10.10.88</td>
<td>100.10.10.2</td>
<td>enabled</td>
<td>up</td>
<td>BDR</td>
</tr>
<tr>
<td>vlan-215</td>
<td>101.10.10.2</td>
<td>0.0.0.0</td>
<td>enabled</td>
<td>up</td>
<td>DR</td>
</tr>
<tr>
<td>vlan-220</td>
<td>10.10.20.1</td>
<td>0.0.0.0</td>
<td>enabled</td>
<td>up</td>
<td>DR</td>
</tr>
<tr>
<td>service-1200</td>
<td>13.1.1.1</td>
<td>13.1.1.2</td>
<td>enabled</td>
<td>UP</td>
<td>BDR</td>
</tr>
<tr>
<td>tunnel-1</td>
<td>10.1.1.2</td>
<td>0.0.0.0</td>
<td>enabled</td>
<td>UP</td>
<td>DR</td>
</tr>
</tbody>
</table>

**output definitions**

- **Interface Name**: The name of the interface.
- **DR Address**: The designated router IP address on this network segment.
- **Backup DR Address**: The IP address of the backup designated router.
- **Admin Status**: The current administration status of the interface, either enabled or disabled.
- **Oper Status**: Whether the interface is an active OSPF interface.
output definitions (continued)

<table>
<thead>
<tr>
<th>State</th>
<th>The current state of the OSPF interface. It will be down, up, dp, dr, or other.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Status</td>
<td>The current status of BFD for the OSPF interface.</td>
</tr>
</tbody>
</table>

The following is an example of MD5 authentication (an interface name is used in this example):

```plaintext
-> show ip ospf interface vlan-213
Interface IP Name = vlan-213
Interface IP Address = 100.10.10.2,
Interface IP Mask = 255.255.255.0,
Domain Name = Vlan,
Domain ID = 213,
Admin Status = Enabled,
Operational Status = Up,
OSPF Interface State = BDR,
Interface Type = Broadcast,
Area Id = 0.0.0.2,
Designated Router IP Address = 100.10.10.88,
Designated Router RouterId = 100.10.10.88,
Backup Designated Router IP Address = 192.169.1.2,
Backup Designated Router RouterId = 192.169.1.2,
MTU (bytes) = 1500,
Metric Cost = 1,
Priority = 1,
Hello Interval (seconds) = 10,
Transit Delay (seconds) = 1,
Retrans Interval (seconds) = 5,
Dead Interval (seconds) = 40,
Poll Interval (seconds) = 120,
Link Type = Broadcast,
Authentication Type = md5,
# of Events = 2,
# of Init State Neighbors = 0,
# of 2-Way State Neighbors = 0,
# of Exchange State Neighbors = 0,
# of Full State Neighbors = 1
BFD status = Disabled,
DR-Only Option for BFD = Disabled
```

The following is an example of simple authentication (an interface name is used in this example):

```plaintext
-> show ip ospf interface vlan-215
Interface IP Name = vlan-215
Interface IP Address = 101.10.10.2,
Interface IP Mask = 255.255.255.0,
Domain Name = Vlan,
Domain ID = 215,
Admin Status = Enabled,
Operational Status = Up,
OSPF Interface State = DR,
Interface Type = Broadcast,
Area Id = 0.0.0.2,
Designated Router IP Address = 101.10.10.88,
Designated Router RouterId = 192.169.1.2,
Backup Designated Router IP Address = 192.169.1.2,
Backup Designated Router RouterId = 192.169.1.2,
MTU (bytes) = 1500,
Metric Cost = 1,
```

The current state of the OSPF interface. It will be down, up, dp, dr, or other.
The current status of BFD for the OSPF interface.
Priority = 1,
Hello Interval (seconds) = 10,
Transit Delay (seconds) = 1,
Retrans Interval (seconds) = 5,
Dead Interval (seconds) = 40,
Poll Interval (seconds) = 120,
Link Type = Broadcast,
Authentication Type = simple,
Authentication Key = Set,
# of Events = 3,
# of Init State Neighbors = 0,
# of Exchange State Neighbors = 0,
# of 2-Way State Neighbors = 0,
# of Full State Neighbors = 0
BFD Status = Disabled,
DR-Only Option for BFD = Disabled

The following is an example of keychain authentication (an interface name is used in this example):
-> show ip ospf interface vlan-220

Interface IP Name = vlan-220,
Interface IP Address = 10.10.20.1,
Interface IP Mask = 255.255.255.0,
Domain Name = Vlan,
Domain ID = 220,
Admin Status = Enabled,
Operational Status = Up,
OSPF Interface State = DR,
Interface Type = Broadcast,
Area Id = 0.0.0.0,
Designated Router IP Address = 10.10.20.1,
Designated Router RouterId = 10.10.10.1,
Backup Designated Router IP Address = 0.0.0.0,
Backup Designated Router RouterId = 0.0.0.0,
MTU (bytes) = 1500,
Metric Cost = 1,
Priority = 1,
Hello Interval (seconds) = 10,
Transit Delay (seconds) = 1,
Retrans Interval (seconds) = 5,
Dead Interval (seconds) = 40,
Poll Interval (seconds) = 120,
Link Type = Broadcast,
Authentication Type = Keychain(1),
# of Events = 2,
# of Init State Neighbors = 0,
# of 2-Way State Neighbors = 0,
# of Exchange State Neighbors = 0,
# of Full State Neighbors = 0,
# of type-9 LSAs on this interface = 0,
BFD status = Disabled,
DR-Only Option for BFD = Disabled

The following are examples of an OSPF interface configured for an IP interface that is bound to a service and configured for an IP interface that is bound to a tunnel (an interface name is used in each example):
-> show ip ospf interface service-1200

Interface IP Name = service-1200,
Interface IP Address = 13.1.1.2,
Interface IP Mask = 255.255.255.0,
Domain Name = Service,
Domain ID = 1200,
Admin Status = Enabled,
Operational Status = Up,
OSPF Interface State = BDR,
Interface Type = Broadcast,
Area Id = 0.0.0.1,
Designated Router IP Address = 13.1.1.1,
Designated Router RouterId = 172.28.4.133,
Backup Designated Router IP Address = 13.1.1.2,
Backup Designated Router RouterId = 2.2.2.2,
MTU (bytes) = 1500,
Metric Cost = 1,
Priority = 1,
Hello Interval (seconds) = 10,
Transit Delay (seconds) = 1,
Retrans Interval (seconds) = 5,
Dead Interval (seconds) = 40,
Poll Interval (seconds) = 120,
Link Type = Broadcast,
Authentication Type = none,
# of Events = 3,
# of Init State Neighbors = 0,
# of 2-Way State Neighbors = 0,
# of Exchange State Neighbors = 0,
# of Full State Neighbors = 1,
# of type-9 LSAs on this interface = 0,
BFD status = Enabled,
DR-Only Option for BFD = Disabled

-> show ip ospf interface tunnel-1
Interface IP Name = tunnel-1,
Interface IP Address = 10.1.1.2,
Interface IP Mask = 255.255.255.0,
Domain Name = Tunnel,
Domain ID = NA,
Admin Status = Enabled,
Operational Status = Up,
OSPF Interface State = DR,
Interface Type = Broadcast,
Area Id = 0.0.0.0,
Designated Router IP Address = 10.1.1.2,
Designated Router RouterId = 20.1.1.1,
Backup Designated Router IP Address = 0.0.0.0,
Backup Designated Router RouterId = 0.0.0.0,
MTU (bytes) = 1480,
Metric Cost = 1,
Priority = 1,
Hello Interval (seconds) = 10,
Transit Delay (seconds) = 1,
Retrans Interval (seconds) = 5,
Dead Interval (seconds) = 40,
Poll Interval (seconds) = 120,
Link Type = Broadcast,
Authentication Type = none,
# of Events = 3,
# of Init State Neighbors = 0,
# of 2-Way State Neighbors = 0,
# of Exchange State Neighbors = 0,
# of Full State Neighbors = 0,
# of type-9 LSAs on this interface = 0,
BFD status = Enabled,
DR-Only Option for BFD = Disabled

Output fields when an interface name is specified are described below:
output definitions

<table>
<thead>
<tr>
<th><strong>Interface IP Name</strong></th>
<th>The name of the IP interface on which OSPF is configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface IP Address</strong></td>
<td>The IP address assigned to the interface.</td>
</tr>
<tr>
<td><strong>Interface IP Mask</strong></td>
<td>The IP mask associated with the IP address assigned to the interface.</td>
</tr>
<tr>
<td><strong>Domain Name</strong></td>
<td>The domain on which the IP interface was configured (VLAN, Service, or Tunnel).</td>
</tr>
<tr>
<td><strong>Domain ID</strong></td>
<td>The VLAN ID or service ID on which the IP interface was configured. This field displays “NA” for IP tunnels.</td>
</tr>
<tr>
<td><strong>Admin Status</strong></td>
<td>The current administration status of the interface (enabled or disabled).</td>
</tr>
<tr>
<td><strong>Operational Status</strong></td>
<td>Whether the interface is an active OSPF interface.</td>
</tr>
<tr>
<td><strong>OSPF Interface State</strong></td>
<td>The current state of the OSPF interface (down, up, dp, dr, or other).</td>
</tr>
<tr>
<td><strong>Interface Type</strong></td>
<td>The OSPF interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.</td>
</tr>
<tr>
<td><strong>Area Id</strong></td>
<td>The area identification number to which the interface is assigned. This field is not applicable if an interface has not yet been assigned to an area.</td>
</tr>
<tr>
<td><strong>Designated Router IP Address</strong></td>
<td>The designated router IP address.</td>
</tr>
<tr>
<td><strong>Designated Router RouterId</strong></td>
<td>The identification number of the designated router.</td>
</tr>
<tr>
<td><strong>Backup Designated Router IP Address</strong></td>
<td>The IP address of the backup designated router.</td>
</tr>
<tr>
<td><strong>Backup Designated Router RouterId</strong></td>
<td>The identification number of the backup designated router.</td>
</tr>
<tr>
<td><strong>MTU</strong></td>
<td>The Maximum Transfer Unit (in bytes) for the interface.</td>
</tr>
<tr>
<td><strong>Metric Cost</strong></td>
<td>The cost added to routes learned on this interface.</td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.</td>
</tr>
<tr>
<td><strong>Hello Interval</strong></td>
<td>The number of seconds between hello messages sent out on the interface.</td>
</tr>
<tr>
<td><strong>Transit Delay</strong></td>
<td>The estimated number of seconds required to transmit a link state update over this interface.</td>
</tr>
<tr>
<td><strong>Retrans Interval</strong></td>
<td>The number of seconds the interface waits before resending hello messages.</td>
</tr>
<tr>
<td><strong>Dead Interval</strong></td>
<td>The number of seconds the interface waits for hello messages received from a neighbor before declaring the neighbor as dead.</td>
</tr>
<tr>
<td><strong>Poll Interval</strong></td>
<td>The larger time interval, in seconds, between hello messages sent to inactive neighbors.</td>
</tr>
<tr>
<td><strong>Link Type</strong></td>
<td>The IP interface type (broadcast or non broadcast).</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>The type of authentication used by this interface (None, Simple, MD5, or Keychain).</td>
</tr>
<tr>
<td><strong>#</strong></td>
<td>The indexing of the MD5 key. (This field is only displayed for MD5 authentication.)</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>A key identifier that identifies the algorithm and MD5 secret key associated with this interface. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>Key</td>
<td>Indicates whether the MD5 key has been set or not. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the configured MD5 authentication key. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>StartAccept</td>
<td>The time that the OSPF router will start accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>StopAccept</td>
<td>The time that the OSPF router will stop accepting packets that have been created with this key. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>StartGen</td>
<td>The time that the OSPF router will start using this key for packet generation. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>StopGen</td>
<td>The time that the OSPF router will stop using this key for packet generation. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>Authentication Key</td>
<td>This field displays whether the authentication key has been configured or not. (This field is only displayed for simple and no authentication.)</td>
</tr>
<tr>
<td># of Events</td>
<td>The number of interface state machine events.</td>
</tr>
<tr>
<td># of Init State Neighbors</td>
<td>The number of OSPF neighbors in the initialization state.</td>
</tr>
<tr>
<td># of 2-Way State Neighbors</td>
<td>The number of OSPF 2-way state neighbors on this interface.</td>
</tr>
<tr>
<td># of Exchange State Neighbors</td>
<td>The number of OSPF neighbors in the exchange state.</td>
</tr>
<tr>
<td># of Full State Neighbors</td>
<td>The number of OSPF neighbors in the full state. The full state is a neighbor that is recognized and passing data between itself and the interface.</td>
</tr>
<tr>
<td># of type-9 LSAs on this interface</td>
<td>Number of type-9 LSA on this interface. (This field is only displayed for keychain authentication.)</td>
</tr>
<tr>
<td>BFD Status</td>
<td>The status of BFD on this interface.</td>
</tr>
<tr>
<td>DR-Only Option for BFD</td>
<td>The BFD setting for this interface. If DR-Only only is disabled then the setting is All Neighbors.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.6R2; “Domain Name” and “Domain ID” fields added.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip ospf interface</code></td>
<td>Creates and deletes an OSPF interface.</td>
</tr>
<tr>
<td><code>ip ospf interface auth-key</code></td>
<td>Configures an OSPF authentication key for simple authentication on an interface.</td>
</tr>
<tr>
<td><code>ip ospf interface dead-interval</code></td>
<td>Configures the OSPF interface dead interval.</td>
</tr>
<tr>
<td><code>ip ospf interface hello-interval</code></td>
<td>Configures the OSPF interface hello interval.</td>
</tr>
<tr>
<td><code>ip ospf interface md5</code></td>
<td>Creates and deletes the OSPF interface MD5 key identification number.</td>
</tr>
<tr>
<td><code>ip ospf interface md5 key</code></td>
<td>Configures the OSPF key string.</td>
</tr>
<tr>
<td><code>ip ospf interface cost</code></td>
<td>Configures the OSPF interface cost.</td>
</tr>
<tr>
<td><code>ip ospf interface poll-interval</code></td>
<td>Configures the OSPF poll interval for a Non Broadcast Multi Access (NBMA) interface.</td>
</tr>
<tr>
<td><code>ip ospf interface priority</code></td>
<td>Configures the OSPF interface priority.</td>
</tr>
<tr>
<td><code>ip ospf interface retrans-interval</code></td>
<td>Configures the OSPF interface retransmit interval.</td>
</tr>
<tr>
<td><code>ip ospf interface transit-delay</code></td>
<td>Configures the OSPF interface transit delay.</td>
</tr>
<tr>
<td><code>ip ospf interface auth-type</code></td>
<td>Sets the OSPF interface authentication type.</td>
</tr>
<tr>
<td><code>ip ospf interface area</code></td>
<td>Configures an OSPF interface area.</td>
</tr>
<tr>
<td><code>ip ospf interface type</code></td>
<td>Configures the OSPF interface type.</td>
</tr>
<tr>
<td><code>ip ospf interface admin-state</code></td>
<td>Enables or disables the administration status on an OSPF interface.</td>
</tr>
<tr>
<td><code>ip ospf interface bfd-state</code></td>
<td>Enables or disables the status of BFD for an OSPF interface.</td>
</tr>
<tr>
<td><code>ip ospf interface bfd-state drs-only</code></td>
<td>Configures whether BFD sessions are only established with neighbors that are in the full state.</td>
</tr>
</tbody>
</table>
**MIB Objects**

ospfIfTable
- ospfIfIpAddress
- ospfIfAreaId
- ospfIfType
- ospfIfAdminStat
- ospfIfRtrPriority
- ospfIfTransitDelay
- ospfIfRetransInterval
- ospfIfHelloInterval
- ospfIfRtrDeadInterval
- ospfIfPollInterval
- ospfIfState
- ospfIfDesignatedRouter
- ospfIfBackupDesignatedRouter
- ospfIfEvents
- ospfIfAuthType
- ospfIfStatus
- ospfIfAuthKey

alaOspfIfMd5Table
- alaOspfIfMd5IpAddress
- alaOspfIfMd5KeyId
- alaOspfIfMd5Key
- alaOspfIfMd5EncryptKey
- alaOspfIfMd5KeyStartAccept
- alaOspfIfMd5KeyStopAccept
- alaOspfIfMd5KeyStartGenerate
- alaOspfIfMd5KeyStopGenerate

alaOspfIfAugTable
- alaOspfIfEncryptKey
- alaOspfIfIpMask
- alaOspfIfDrRouterid
- alaOspfIfBdrRouterid
- alaOspfIfMTU
- alaOspfIfInitNbrs
- alaOspfIfExchNbrs
- alaOspfIfFullNbrs
- alaOspfIfLinkType
- alaOspfIfOperStatus
- alaOspfIfIntfName
- alaOspfIf2WayNbrs
- alaOspfIfBfdStatus
- alaOspfIfBfdDrsOnly
- alaOspfIfKeyChainId
- alaOspfIfIntfIndex
**show ip ospf interface auth-info**

Displays authentication information for the interface.

```
show ip ospf interface auth-info [interface_name]
```

**Syntax Definitions**

`interface_name` The name of the interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Not specifying an interface name displays all known interfaces for the OSPF router.
- When keychain authentication type is used for the interface, only the keychain ID is displayed. To view the keys associated with the keychain, use the keychain commands. For more information on keychain management commands, refer to the “Chassis Management and Monitoring Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.

**Examples**

```
-> show ip ospf interface auth-info

Interface Name       Key-chain KeyId Key   Status   AuthMode
---------------------+------------+-------+--------+----------+-----------
               vlan-30-int        1     --     --      Enabled keychain
               vlan-20-int       --     10     Set     Enabled Keyed-MD5
```

**output definitions**

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>The name of the interface.</td>
</tr>
<tr>
<td>Key-chain</td>
<td>The keychain associated with the interface.</td>
</tr>
<tr>
<td>KeyId</td>
<td>A key identifier that identifies the algorithm and MD5 secret key associated with this interface. (This field is only displayed for MD5 authentication.)</td>
</tr>
<tr>
<td>Key</td>
<td>Indicates whether the key has been set or not.</td>
</tr>
</tbody>
</table>
OSPF Commands

show ip ospf interface auth-info

output definitions (continued)

<table>
<thead>
<tr>
<th>Status</th>
<th>The current administration status of the interface, either enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthMode</td>
<td>The type of authentication used by this interface.</td>
</tr>
</tbody>
</table>

Release History

Release 8.4.1; command introduced.

Related Commands

ip ospf interface auth-type

Sets the OSPF interface authentication type. Authentication allows the router to only respond to other routers that have the correct authentication information.

MIB Objects

N/A
**show ip ospf restart**

Displays the OSPF graceful restart related configuration and status.

```
show ip ospf restart
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The minimum hardware configuration for this command is a redundant CMM configuration.

### Examples

```
-> show ip ospf restart
Restart Support = Enabled,
Restart Interval (in seconds) = 120,
Restart Status = Not Restarting,
Restart Age (in seconds) = 0,
Last Restart Exit Reason = None,
Restart Helper Support = Enabled,
Restart Helper Strict Checking = Enabled,
Restart Helper Mode = NotHelping
```

### output definitions

- **Restart Support**: The administrative status of OSPF graceful restart, which can be **Enabled** or **Disabled**.
- **Restart Interval**: The configured OSPF hitless restart timeout interval, in seconds. Use the `ip ospf restart-interval` command to modify this parameter.
- **Restart Status**: The current status of OSPF graceful restart, which can be **Not Restarting**, **Unplanned Restart** (after a CMM takeover), or **Planned Restart** (before CMM takeover).
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restart Age</strong></td>
<td>The remaining time, in seconds, for the current OSPF graceful restart interval.</td>
</tr>
<tr>
<td><strong>Last Restart Exit Reason</strong></td>
<td>The outcome of the last attempt at a graceful restart. If the value is None, then no restart has yet been attempted. If the value is In Progress, then a restart attempt is currently underway. Other possible values include Completed (successfully completed), Timed Out (timed out), and Topology Changed (aborted due to topology change).</td>
</tr>
<tr>
<td><strong>Restart Helper Support</strong></td>
<td>The administrative status of the capability of an OSPF router to operate in helper mode in response to a router performing a graceful restart, which can be Enabled or Disabled. Use the ip ospf restart-helper admin-state command to modify this parameter.</td>
</tr>
<tr>
<td><strong>Restart Helper Strict Checking</strong></td>
<td>The administrative status of whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router, which can be Enabled or Disabled. Use the ip ospf restart-helper strict-lsa-checking admin-state command to modify this parameter.</td>
</tr>
<tr>
<td><strong>Restart Helper Mode</strong></td>
<td>Whether this OSPF router is operating as a helper to a restarting router.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip ospf restart-support** Configures support for the graceful restart feature on an OSPF router.
- **ip ospf restart initiate** Initiates a planned graceful restart.

**MIB Objects**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
Open Shortest Path First version 3 (OSPFv3) routing is a shortest path first (SPF) or link-state protocol. This protocol is compatible with 128-bit IPv6 address space, while OSPF is compatible with 32-bit IPv4 address space. OSPFv3 is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS). OSPFv3 chooses the least-cost path as the best path.

Each participating router distributes its local state (i.e., the router’s usable interfaces and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. This database is built from the collected link state advertisements of all routers. Each multi-access network that has at least two attached routers has a designated router and a backup designated router. The designated router floods a link state advertisement for the multi-access network and has other special responsibilities.

OSPFv3 allows collections of contiguous networks and hosts to be grouped together. A group, together with the routers having interfaces to any one of the included networks, is called an area. Each area runs a separate copy of the basic link-state routing algorithm. This means that each area has its own topological database, as explained in the previous section.

The OmniSwitch version of OSPFv3 complies with RFCs 2740, 1826, 1827, 2553, 2373, 2374, and 2460.

MIB information for OSPFv3 is as follows:

- **Filename:** ALCATEL-IND1-VIRTUALROUTER-MIB.mib
  **Module:** alcatelIND1VirtualRouterMIB

- **Filename:** ALCATEL-IND1-OSPF3-MIB.mib
  **Module:** alcatelIND1OSPF3MIB

- **Filename:** OSPFV3-MIB.mib
  **Module:** ospfv3MIB
The following is a list of the commands for configuring OSPFv3:

| Global OSPFv3 Commands       | ipv6 load ospf               |
|                              | ipv6 ospf admin-state        |
|                              | ipv6 ospf host               |
|                              | ipv6 ospf mtu-checking       |
|                              | ipv6 ospf route-tag          |
|                              | ipv6 ospf spf-timer          |
|                              | ipv6 ospf virtual-link       |
|                              | show ipv6 ospf               |
|                              | show ipv6 ospf border-routers|
|                              | show ipv6 ospf host          |
|                              | show ipv6 ospf lsdb          |
|                              | show ipv6 ospf neighbor      |
|                              | show ipv6 ospf routes        |
|                              | show ipv6 ospf virtual-link  |

| OSPFv3 Area Commands         | ipv6 ospf area               |
|                              | ipv6 ospf area area-summary  |
|                              | ipv6 ospf area nssa-translator-role |
|                              | ipv6 ospf area nssa-translator-stab-interval |
|                              | ipv6 ospf area nssa-summarize |
|                              | show ipv6 ospf area          |

| OSPFv3 Interface Commands    | ipv6 ospf interface          |
|                              | ipv6 ospf interface admin-state |
|                              | ipv6 ospf interface suppress-link-lsa |
|                              | ipv6 ospf interface type      |
|                              | ipv6 ospf neighbor            |
|                              | ipv6 ospf interface area      |
|                              | ipv6 ospf interface dead-interval |
|                              | ipv6 ospf interface hello-interval |
|                              | ipv6 ospf interface cost      |
|                              | ipv6 ospf interface priority  |
|                              | ipv6 ospf interface retrans-interval |
|                              | ipv6 ospf interface transit-delay |
|                              | show ipv6 ospf interface      |

| OSPFv3 BFD Commands          | ipv6 ospf bfd-state          |
|                              | ipv6 ospf bfd-state all-interfaces |
|                              | ipv6 ospf interface bfd-state |
|                              | ipv6 ospf interface bfd-state drs-only |
|                              | ipv6 ospf interface bfd-state all-neighbors |

| OSPFv3 Graceful Restart Commands | ipv6 ospf restart          |
|                                  | ipv6 ospf restart initiate |
|                                  | ipv6 ospf restart interval  |
|                                  | ipv6 ospf restart-helper    |
|                                  | ipv6 ospf restart-helper strict-lsa-check |
|                                  | show ipv6 ospf restart      |
ipv6 load ospf

Loads the OSPFv3 software on the router.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Example

-> ipv6 load ospf

Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

alaVrConfigTable
  alaVrConfigOspf3Status
**ipv6 ospf admin-state**

Enables or disables the OSPFv3 administrative status for the router.

`ipv6 ospf admin-state {enable | disable}`

---

**Syntax Definitions**

| enable | Specifies enable option.
|--------|-------------------|
| disable| Specifies disable option.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The OSPFv3 protocol should be enabled to route traffic.

**Examples**

-> `ipv6 ospf admin-state enable`

-> `ipv6 ospf admin-state disable`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`show ipv6 ospf` Displays OSPFv3 status and general configuration parameters.

**MIB Objects**

- `ospfv3GeneralGroup`
- `ospfv3AdminStat`
**ipv6 ospf host**

Creates or deletes an OSPFv3 entry for directly attached hosts.

```plaintext
ipv6 ospf host ipv6_address [area area_id] [metric metric]
no ipv6 ospf host ipv6_address area area_id
```

**Syntax Definitions**

- `ipv6_address`: The 128-bit IP address of the OSPFv3 host.
- `area_id`: Area to which the host route belongs.
- `metric`: The cost metric value assigned to the specified host. The valid range is 0–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove the record of the OSPFv3 host.
- Use this command when multiple paths exist to a host. The specified host must be directly attached to the router. A metric value is the cost of all the hops necessary for a packet to reach its destination. Routers use the metric to determine the best possible path.
- This command allows you to modify the host parameter `metric`.

**Examples**

```plaintext
- ipv6 ospf host 2001::1/64 metric 10
- no ipv6 ospf host 2001::1/64 metric 10
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ipv6 ospf host

Displays information on the configured OSPFv3 hosts.

MIB Objects

ospfv3HostTable

ospfv3HostStatus
ospfv3HostAreaID
ospfv3HostAddress
ospfv3HostMetric
ipv6 ospf mtu-checking

Enables or disables Maximum Transfer Unit (MTU) checking. The MTU limits the size of a transmitted or received packet.

*ipv6 ospf mtu-checking*

*no ipv6 ospf mtu-checking*

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to disable MTU checking.

- This command is used to disable the checking for mismatch of the interface MTU while establishing a neighbor adjacency with a router. MTU mismatch occurs when a router receives packets that contain a larger MTU value than that of the interface on which adjacency is being established. The interface MTU is the largest IP datagram size (in bytes) that the interface can accept.

**Examples**

```
-> ipv6 ospf mtu-checking
-> no ipv6 ospf mtu-checking
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ipv6 ospf
Displays the OSPFv3 status and general configuration parameters.

MIB Objects

alaProtocolOspf3
alaOspf3MTUCheck
ipv6 ospf route-tag

Configures a tag value for the Autonomous System External (ASE) routes created.

ipv6 ospf route-tag tag

Syntax Definitions

tag The set tag value. The valid range is 0–2, 147, 483, 647.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag</td>
<td>0</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>platforms</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command allows you to set a tag value for ASE routes that are learned by this OSPFv3 router. The tag value allows for quick identification.
- OSPFv3 ASE route advertisements contain a tag value field. This field allows the exchange of information between autonomous system border routers (ASBRs).

Examples

-> ipv6 ospf route-tag 2

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf Displays OSPFv3 status and general configuration parameters.

MIB Objects

alaProtocolOspf3
alaOspf3RedistRouteTag
**ipv6 ospf spf-timer**

Configures timers for Shortest Path First (SPF) calculation.

**ipv6 ospf spf-timer [delay delay_seconds] [hold hold_seconds]**

---

**Syntax Definitions**

- **delay_seconds**: Specifies time (from 0 to 65535 seconds) between the reception of an OSPFv3 topology change and the start of an SPF calculation.
- **hold_seconds**: Specifies the minimum time (from 0 to 65535 seconds) between consecutive SPF calculations.

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>delay_seconds</td>
<td>5</td>
</tr>
<tr>
<td>hold_seconds</td>
<td>10</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command allows you to configure the time interval between SPF calculations.
- Use the delay timer to determine how much time to postpone an SPF calculation after the router receives a topology change.
- Use the hold timer to configure the amount of time that must elapse between consecutive SPF calculations.
- There will be no delay in the SPF calculation if either the delay timer or hold timer is set to 0. The SPF calculations will occur immediately upon the reception of a topology change and/or that back-to-back SPF calculations can take place with no break in-between the two.

---

**Examples**

```
-> ipv6 ospf spf-timer delay 20 hold 35
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ipv6 ospf

Displays the OSPFv3 status and general configuration parameters.

MIB Objects

alaProtocolOspf3

alaOspf3TimerSpfDelay
alaOspf3TimerSpfHold
**ipv6 ospf virtual-link**

Creates or deletes a virtual link. A virtual link restores the backbone connectivity if the backbone is not physically contiguous.

```
ipv6 ospf virtual-link area_area_id router_router_id [dead-interval seconds] [hello-interval seconds] [retrans-interval seconds] [transit-delay seconds]
```

```
no ipv6 ospf virtual-link area_area_id router_router_id
```

### Syntax Definitions

- `area_id` - A unique 32-bit value in IP address format.
- `router_id` - A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
- `dead-interval seconds` - Sets the virtual link dead interval. If no hello packets on this link for the set number of seconds have been received, the virtual neighbor is declared dead. The valid range is 1–2147483647.
- `hello-interval seconds` - Sets the virtual link hello interval, which is the time interval between OSPFv3 hellos sent on this virtual link. The valid range is 1–65535.
- `retrans-interval seconds` - Sets the virtual link retransmit interval. The router waits the set number of seconds before retransmitting OSPFv3 packets. The valid range is 0–3600.
- `transit-delay seconds` - Sets the virtual link transit delay, which is the number of seconds to transmit OSPFv3 packets over this link. The valid range is 0–3600.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dead-interval seconds</code></td>
<td>40</td>
</tr>
<tr>
<td><code>hello-interval seconds</code></td>
<td>10</td>
</tr>
<tr>
<td><code>retrans-interval seconds</code></td>
<td>5</td>
</tr>
<tr>
<td><code>transit-delay seconds</code></td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to delete the virtual link.
• You can define areas in such a way that the backbone is no longer contiguous. In this case, the system administrator can ensure backbone connectivity physically.

• Virtual links can be configured between any two backbone routers that have an interface to a common non-backbone area. Virtual links belong to the backbone. The protocol treats two routers joined by a virtual link as if they were connected by an unnumbered point-to-point network. The routing protocol traffic that flows along the virtual link uses intra-area routing only.

• If authentication is enabled, both routers at either end of the virtual link must share the same password. Simple authentication refers to the use of only clear-text passwords as an authentication method. MD5 authentication refers to the usage of message digests.

• The **dead-interval** value should be the same for all the routers on the same network. This value should be a multiple of the value provided for the **hello-interval**.

**Examples**

-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115
dead-interval 50
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 hello-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 retrans-interval 20
-> ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115 transit-delay 50
-> no ipv6 ospf virtual-link area 0.0.0.1 router 172.22.2.115

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**show ipv6 ospf virtual-link** Displays the virtual link information.

**MIB Objects**

ospfv3VirtIfTable
  ospfv3VirtIfAreaId
  ospfv3VirtIfNeighbor
  ospfv3VirtIfStatus
  ospfv3VirtIfRtrDeadInterval
  ospfv3VirtIfHelloInterval
  ospfv3VirtIfRetransInterval
  ospfv3VirtIfTransitDelay
**ipv6 ospf area**

Assigns an OSPFv3 interface to a specified area.

`ipv6 ospf area area_id [type {normal | stub [default-metric metric] | nssa [default-metric metric]}] [summarize [filter]]`

`no ipv6 ospf area area_id`

---

**Syntax Definitions**

- **area_id**: A unique 32-bit value in IP address format or a unique identification number in the range 0 to 4294967295.
- **normal**: Sets the area as a regular OSPFv3 area.
- **stub**: Configures an OSPFv3 area as a stub area.
- **nssa**: Configures an OSPFv3 area as a NSSA (Not-So-Stubby Area).
- **metric**: Defines the metric to be used for default routes injected into the stub or NSSA. The range is 0 to 4294967295.
- **summarize**: Configures the inter-area route summarization. Prefixes that fall within the summary range can be shared with another area through the summary prefix.
- **filter**: Configure to filter the routes specified in the summarization range. These filtered routes are not advertised into another area.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>stub</td>
<td>normal</td>
</tr>
<tr>
<td>nssa</td>
<td>normal</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to delete the OSPFv3 area.
- To change the area type, first delete the area, and then recreate it with the new type.
- The `default-metric` parameter defines the metric to be used for default routes injected into the stub or NSSA.
- The OS6560 supports stub area only.
**Examples**

- `ipv6 ospf area 0.0.0.1`
- `ipv6 ospf area 0.0.0.1 stub default-metric 15`
- `ipv6 ospf area 0.0.0.1 type normal`
- `ipv6 ospf area 0.0.0.1 type nssa`
- `ipv6 ospf area 0.0.0.1 summarize 2001:1::/64`
- `no ipv6 ospf area 0.0.0.1`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; nssa keyword added.

**Related Commands**

- `show ipv6 ospf area` Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

**MIB Objects**

- `ospfv3AreaTable`
  - `ospfv3ImportAsExtern`
  - `ospfv3AreaSummary`
  - `ospfv3StubMetric`
  - `ospfv3AreaId`
  - `ospfv3AreaImportAsExtern`
**ipv6 ospf area area-summary**

Configures whether or not summary routes are imported into the stub or NSSA as Type-3 summary-LSAs.

```
ipv6 ospf area area_id [area-summary {noareasummary | sendareasummary}]
```

---

**Syntax Definitions**

- `area_id` The area ID configured for a stub or NSSA.
- `noareasummary` When set to this option, inter-area LSAs will neither originate or propagate into the NSSA. Only a default route will be advertised into the NSSA.
- `sendareasummary` When set to this option, inter-area LSAs will be summarized and propagated into the NSSA.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>noareasummary</td>
<td>sendareasummary</td>
</tr>
<tr>
<td>sendareasummary</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> ipv6 ospf area 0.0.0.1 area-summary noAreaSummary
```

**Release History**

Release 8.4.1; command introduced.
Related Commands

- **ipv6 ospf area** Assigns an OSPFv3 interface to a specified area.
- **show ipv6 ospf area** Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

MIB Objects

- **ospfv3AreaSummary**
**ipv6 ospf area nssa-translator-role**

Configures whether or not an NSSA border router will unconditionally translate Type-7 LSAs into Type-5 LSAs.

```
ipv6 ospf area area_id [nssa-translator-role {always | candidate}]
```

---

**Syntax Definitions**

- **area_id**: A unique 32-bit value in IP address format.
- **always**: When set to this option, NSSA border router always translates Type-7 LSAs into Type-5 LSAs regardless of the translator state of other NSSA border routers.
- **candidate**: When set to this option, NSSA border router participates in the translator election process.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>candidate</td>
</tr>
</tbody>
</table>

default

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
  No  No Yes No  Yes  Yes  Yes  Yes  Yes  Yes
```

---

**Usage Guidelines**

When translator role is set to **candidate**, NSSA border router invokes a translator election process. The translator is then established by the NSSA border router whose router LSA has the greatest router ID.

---

**Examples**

```
-> ipv6 ospf area 0.0.0.1 nssa-translator role always
```

---

**Release History**

Release 8.4.1; command introduced.
**Related Commands**

- **ipv6 ospf area**
  Assigns an OSPFv3 interface to a specified area.

- **show ipv6 ospf area**
  Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

**MIB Objects**

- `ospfv3AreaNssaTranslatorRole`
**ipv6 ospf area nssa-translator-stab-interval**

Configures the duration for which a Type-7 translator will continue in the translator role after another NSSA border router translator has assumed the role.

`ipv6 ospf area area_id [nssa-translator-stab-interval interval]`

**Syntax Definitions**

- **area_id**: A unique 32-bit value in IP address format.
- **interval**: NSSA translator stability interval value in seconds. The range is 0 to 4294967295.

**Defaults**

The default value is 40 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> ipv6 ospf area 0.0.0.1 nssa-translator-stab-interval 60`

**Release History**

Release 8.4.1; command introduced.

**Related Commands**

- `ipv6 ospf area`: Assigns an OSPFv3 interface to a specified area.
- `show ipv6 ospf area`: Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

**MIB Objects**

- `ospfv3AreaNssaTranslatorStabInterval`
**ipv6 ospf area nssa-summarize**

Configures an NSSA summary of IPv6 prefix in the given area. Any NSSA LSAs within the area subsumed by IPv6 prefix will be summarized into other areas as an external LSA with a prefix of IPv6 prefix.

```
ipv6 ospf area area_id nssa-summarize ipv6_address_prefix [filter]
```

### Syntax Definitions

- **area_id**: A unique 32-bit value in IP address format.
- **ipv6_address_prefix**: The 128-bit IPv6 address in hexadecimal format.
- **filter**: Use filter option to suppress the external LSA.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> ipv6 ospf area 2 nssa-summarize c000::/64
```

### Release History

Release 8.4.1 R03; command introduced.

### Related Commands

- **ipv6 ospf area**: Assigns an OSPFv3 interface to a specified area.
- **show ipv6 ospf area**: Displays either all the OSPFv6 areas, or a specified OSPFv6 area.

### MIB Objects

- `ospfv3AreaAggregateTable`
ipv6 ospf interface

Creates or deletes an OSPFv3 interface.

ipv6 ospf interface interface_name

no ipv6 ospf interface interface_name

Syntax Definitions

interface_name The name of the interface.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of the command to delete an OSPFv3 interface.
- The interface name cannot contain spaces.

Examples

-> ipv6 ospf interface vlan-101
-> no ipv6 ospf interface vlan-101

Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 ospf interface Displays the status and statistics of an OSPFv3 interface.

MIB Objects

ospfv3IfTable
ospfv3IfIndex
**ipv6 ospf interface admin-state**

Enables or disables the administration status on an OSPFv3 interface.

```
ipv6 ospf interface interface_name admin-state {enable | disable}
no ipv6 ospf interface interface_name
```

### Syntax Definitions

- **interface_name**: The name of the interface.
- **enable**: Enables the OSPFv3 interface.
- **disable**: Disables the OSPFv3 interface.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to delete an OSPFv3 interface.
- The OSPFv3 interface must be enabled to participate in the OSPFv3 protocol.

### Examples

```
-> ipv6 ospf interface vlan-101 admin-state enable
-> ipv6 ospf interface vlan-101 admin-state disable
-> no ipv6 ospf interface vlan-101
-> no ipv6 ospf interface vlan-101
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

show ipv6 ospf interface  
Displays the status and statistics of an OSPFv3 interface.

MIB Objects

ospfv3IfTable
  ospfv3IfIndex
  ospfv3IfAdminStat
**ipv6 ospf interface suppress-link-lsa**

Allows to suppress the announcements of the Link State Advertisements (LSAs).

```
ipv6 ospf interface interface_name suppress-link-lsa
```

```
no ipv6 ospf interface interface_name suppress-link-lsa
```

**Syntax Definitions**

```
interface_name
```

The name of the interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of the command to disable LSA suppression.

**Examples**

```
-> ipv6 ospf interface vlan-101 suppress-link-lsa
-> no ipv6 ospf interface vlan-101 suppress-link-lsa
```

**Release History**

Release 8.1.1; command introduced.

**Related Commands**

**show ipv6 ospf interface**

Displays the status and statistics of an OSPFv3 interface.

**MIB Objects**

`ospfv3IfTable`

`ospfv3IfIndex`

`alaOspf3SuppressLinkLsa`
ipv6 ospf interface type

Allows to configure the type of OSPFv3 interface.

ipv6 ospf interface interface_name type {broadcast | point-to-point | point-to-multipoint | nbma}

Syntax Definitions

- **interface_name**: The name of the interface.
- **broadcast**: The interface is a broadcast interface.
- **point-to-point**: The interface is a point-to-point interface.
- **point-to-multipoint**: The interface is a point-to-multipoint interface.
- **nbma**: The interface is a NBMA interface.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>broadcast</td>
</tr>
<tr>
<td>point-to-point</td>
<td>broadcast</td>
</tr>
<tr>
<td>point-to-multipoint</td>
<td>broadcast</td>
</tr>
<tr>
<td>nbma</td>
<td>broadcast</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The OSPFv3 interface must be enabled to participate in the OSPFv3 protocol.

Examples

- `ipv6 ospf interface vlan-101 type nbma`
- `ipv6 ospf interface vlan-101 type point-to-point`
- `ipv6 ospf interface vlan-101 type point-to-multipoint`
- `ipv6 ospf interface vlan-101 type broadcast`

Release History

Release 8.1.1; command introduced.
**Related Commands**

`show ipv6 ospf interface`  Displays the status and statistics of an OSPFv3 interface.

**MIB Objects**

ospfv3IfTable
  ospfv3IfStatus
  ospfv3IfType
**ipv6 ospf neighbor**

Allows to configure OSPFv3 neighbor on non-broadcast interface type. The neighbor configuration is required on NBMA and point-to-multipoint interface to run OSPFv3.

```
ipv6 ospf neighbor nbr_ipv6_address interface interface_name {eligible | ineligible}
no ipv6 ospf neighbor nbr_ipv6_address
```

### Syntax Definitions

- **nbr_ipv6_address**: Link-local address of the neighbor to be linked.
- **interface_name**: The name of the interface on which the neighbor is reachable.
- **eligible**: Indicates the neighbor is eligible to become the designated router.
- **ineligible**: Indicates the neighbor is ineligible to become the designated router.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>eligible</td>
<td>ineligible</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C8/C32E/T24C2/ X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of the command to delete the neighbor configuration.
- The OSPFv3 interface must be configured before configuring the OSPFv3 neighbor.
- This command is not applicable for broadcast interface type and is optional for point-to-point interface type.

### Examples

```
-> ipv6 ospf neighbor fe80::2e0:blff:fe7e:5f1e interface vlan-101 eligible
-> ipv6 ospf neighbor fe80::2e0:blff:fe7e:5f1e interface vlan-101 ineligible
-> no ipv6 ospf neighbor fe80::2e0:blff:fe7e:5f1e interface vlan-101
```

### Release History

Release 8.1.1; command introduced.
**Related Commands**

`show ipv6 ospf interface` Displays the status and statistics of an OSPFv3 interface.
`ipv6 ospf interface admin-state` Allows to configure the type of OSPFv3 interface.

**MIB Objects**

`ospfv3NbrTable`
  `ospfv3NbrPriority`
  `ospfv3NbmaNbrStatus`
**ipv6 ospf interface area**

Configures an OSPFv3 area identifier for this interface.

```
ipv6 ospf interface interface_name area area_id
```

### Syntax Definitions

- **interface_name**  The name of the interface.
- **area_id**  A unique 32-bit value in IP address format.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

An interface must be assigned to an area to become operational.

### Examples

```
-> ipv6 ospf interface vlan-101 area 0.0.0.1
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **show ipv6 ospf area**  Displays either all the OSPFv3 areas, or a specified OSPFv3 area.
- **show ipv6 ospf interface**  Displays the status and statistics of an OSPFv3 interface.

### MIB Objects

- **ospfv3IfTable**
  - **ospfv3IfIndex**
  - **ospfv3IfAreaId**
ipv6 ospf interface dead-interval

Configures the OSPFv3 interface dead interval.

`ipv6 ospf interface interface_name dead-interval seconds`

**Syntax Definitions**

- `interface_name`: The name of the interface.
- `seconds`: The dead interval, in seconds. The valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>40</td>
</tr>
<tr>
<td>(broadcast and point-to-point)</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td>120</td>
</tr>
<tr>
<td>(NBMA and point-to-multipoint)</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- After the dead interval, a neighbor on this interface is considered dead if no hello packets have been received from this neighbor.
- This interval should be greater than the hello interval or multiples of the hello interval.

**Examples**

```
-> ipv6 ospf interface vlan-101 dead-interval 50
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ipv6 ospf interface hello-interval**  
  Configures the OSPFv3 interface hello interval.

- **show ipv6 ospf interface**  
  Displays the status and statistics of an OSPFv3 interface.

**MIB Objects**

- ospfv3IfTable

  - ospfv3IfIndex
  - ospfv3IfRtrDeadInterval
**ipv6 ospf interface hello-interval**

Configures the OSPFv3 interface hello interval.

```
ipv6 ospf interface interface_name hello-interval seconds
```

**Syntax Definitions**

- `interface_name` The name of the interface.
- `seconds` The hello interval, in seconds. The valid range is 0–65535. A value of 0 creates a passive OSPFv3 interface.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>10</td>
</tr>
<tr>
<td>(broadcast and point-to-point)</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
<tr>
<td>(NBMA and point-to-multipoint)</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This is the interval between two consecutive hello packets sent out on this interface.

**Examples**

```
-> ipv6 ospf interface vlan-101 hello-interval 50
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ipv6 ospf interface dead-interval**  
  Configures the OSPFv3 interface dead interval.

- **show ipv6 ospf interface**  
  Displays the status and statistics of an OSPFv3 interface.

**MIB Objects**

ospfv3IfTable

  ospfv3IfIndex

  ospfv3IfHelloInterval
**ipv6 ospf interface cost**

Configures the OSPFv3 interface cost.

```
ipv6 ospf interface interface_name cost cost
```

**Syntax Definitions**

- `interface_name` The name of the interface.
- `cost` The interface cost. The valid range is 0–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The configured interface cost (if any) is used during OSPFv3 route calculations.

**Examples**

```
-> ipv6 ospf interface vlan-101 cost 10
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ipv6 ospf interface` Displays the status and statistics of an OSPFv3 interface.

**MIB Objects**

- `ospfv3IfTable`
  - `ospfv3IfIndex`
  - `ospfv3IfMetricValue`
**ipv6 ospf interface priority**

Configures the OSPFv3 interface priority. The priority number helps determine the eligibility of this router to become the designated router on the network.

```
ip ospf interface interface_name priority priority
```

**Syntax Definitions**

- `interface_name`: The name of the interface.
- `priority`: The interface priority. The valid range is 0–255.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When two routers attached to a network both attempt to become the designated router, the one with the highest priority becomes the designated router. A router whose router priority is set to 0 is ineligible to become the designated router.

**Examples**

```
-> ipv6 ospf interface vlan-101 priority 100
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 ospf interface* Displays the status and statistics of an OSPFv3 interface.

**MIB Objects**

ospfv3IfTable

  - ospfv3IfIndex
  - ospfv3IfRtrPriority
**ipv6 ospf interface retrans-interval**

Configures the OSPFv3 interface retransmit time interval.

```
ipv6 ospf interface interface_name retrans-interval interval
```

**Syntax Definitions**

- `interface_name` The name of the interface.
- `seconds` The retransmit interval, in seconds. The valid range 0–3600.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval</td>
<td>5</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The number of seconds between link retransmission of OSPFv3 packets on this interface.

**Examples**

```
-> ipv6 ospf interface vlan-101 retrans-interval 500
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ipv6 ospf interface` Displays the status and statistics of an OSPFv3 interface.

**MIB Objects**

- `ospfv3IfTable` (part of `ospfv3IfTable`)
  - `ospfv3IfIndex` (part of `ospfv3IfTable`)
  - `ospfv3IfRetransInterval` (part of `ospfv3IfTable`)
**ipv6 ospf interface transit-delay**

Configures the OSPFv3 interface transit time delay.

```
ipv6 ospf interface interface_name transit-delay delay
```

### Syntax Definitions

- `interface_name` - The name of the interface.
- `delay` - The transit delay, in seconds. The valid range is 0–3600.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The estimated number of seconds required to transmit a link state update over this interface. This command takes into account transmission and propagation delays and must be greater than 0.

### Examples

```
-> ipv6 ospf interface vlan-101 transit-delay 100
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show ipv6 ospf interface` - Displays the status and statistics of an OSPFv3 interface.

### MIB Objects

- `ospfv3IfTable`
  - `ospfv3IfIndex`
  - `ospfv3IfTransitDelay`
**ipv6 ospf bfd-state**

Enables or disables the registration of OSPFv3 with the BFD protocol.

`ipv6 ospf bfd-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for OSPFv3.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for OSPFv3.</td>
</tr>
</tbody>
</table>

---

**Defaults**

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>disable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- BFD must be globally enabled for the switch and OSPFv3 must be registered with BFD at the protocol level before OSPFv3 can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and the OSPFv3 protocol acts based upon the BFD message.
- Whenever a neighbor goes down, OSPFv3 will inform BFD to remove that neighbor from the BFD active list.

---

**Examples**

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of OSPFv3 with the BFD protocol:

```
-> ipv6 ospf bfd-state enable
-> ipv6 ospf bfd-state disable
```

---

**Release History**

Release 8.4.1.R03; command was introduced.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip bfd admin-state</code></td>
<td>Enables or disables the global BFD protocol status for the switch.</td>
</tr>
<tr>
<td><code>ipv6 ospf bfd-state all-interfaces</code></td>
<td>Enables or disables BFD for all OSPFv3 interfaces configured.</td>
</tr>
<tr>
<td><code>ipv6 ospf interface bfd-state</code></td>
<td>Enables or disables BFD for a specific OSPFv3 interface.</td>
</tr>
<tr>
<td><code>ipv6 ospf interface bfd-state drs-only</code></td>
<td>Establishes BFD sessions only on neighbors in full state.</td>
</tr>
<tr>
<td><code>ipv6 ospf interface bfd-state all-neighbors</code></td>
<td>Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.</td>
</tr>
<tr>
<td><code>show ipv6 ospf</code></td>
<td>Displays OSPFv3 status and general configuration parameters.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- `alaProtocolOspf3`  
  - `alaOspf3BfdStatus`
ipv6 ospf bfd-state all-interfaces

Enables or disables BFD for all OSPFv3 interfaces in the switch configuration.

ipv6 ospf bfd-state all-interfaces {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for all the OSPFv3 interfaces.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for all the OSPFv3 interfaces.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

Examples

- `-> ipv6 ospf bfd-state all-interfaces enable`
- `-> ipv6 ospf bfd-state all-interfaces disable`

Release History

Release 8.4.1.R03; command was introduced.
**Related Commands**

- `ipv6 ospf bfd-state` Enables or disables the BFD status for the OSPFv3 protocol.
- `ipv6 ospf interface bfd-state` Enables or disables BFD for a specific OSPFv3 interface.
- `ipv6 ospf interface bfd-state drs-only` Establishes BFD sessions only on neighbors in full state.
- `ipv6 ospf interface bfd-state all-neighbors` Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
- `show ipv6 ospf interface` Displays configuration information for an OSPFv3 interface.

**MIB Objects**

- `alaProtocolOspf3` AOS release 8
- `alaOspf3BfdAllInterfaceStatus`
ipv6 ospf interface bfd-state

Enables or disables BFD for a specific OSPFv3 interface.

ipv6 ospf interface if_name bfd-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_name</td>
<td>The name of an existing OSPFv3 interface.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables BFD for the OSPFv3 interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for the OSPFv3 interface.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

Examples

- ipv6 ospf interface int1 bfd-state enable
- ipv6 ospf interface int2 bfd-state disable

Release History

Release 8.4.1.R03; command was introduced.
**Related Commands**

- `ipv6 ospf bfd-state` Enables or disables the BFD status for the OSPFv3 protocol.
- `ipv6 ospf bfd-state all-interfaces` Enables or disables BFD for all OSPFv3 interfaces configured.
- `ipv6 ospf interface bfd-state drs-only` Establishes BFD sessions only on neighbors in full state.
- `ipv6 ospf interface bfd-state all-neighbors` Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.
- `show ipv6 ospf interface` Displays configuration information for an OSPFv3 interface.

**MIB Objects**

- `alaOspf3IfAugTable`  
  `alaOspf3IfBfdStatus`
**ipv6 ospf interface bfd-state drs-only**

Establishes BFD sessions only with neighbors that are in the full state.

`ipv6 ospf interface if_name bfd-state drs-only`

**Syntax Definitions**

*if_name*  
The name of an existing OSPFv3 interface.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>drs-only</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The specified OSPFv3 interface must be enabled to interact with BFD.
- The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

**Examples**

```
-> ipv6 ospf interface int1 bfd-state drs-only
```

**Release History**

Release 8.4.1.R03; command was introduced.
**Related Commands**

- **ipv6 ospf bfd-state**
  Enables or disables the BFD status for OSPFv3 protocol.

- **ipv6 ospf bfd-state all-interaces**
  Enables or disables BFD for all OSPFv3 interfaces configured.

- **ipv6 ospf interface bfd-state**
  Enables or disables BFD for a specific OSPFv3 interface.

- **ipv6 ospf interface bfd-state all-neighbors**
  Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

- **show ipv6 ospf interface**
  Displays configuration information for an OSPFv3 interface.

**MIB Objects**

- `alaOspf3IfAugTable`
- `alaOspf3IfDrsOnly`
**ipv6 ospf interface bfd-state all-neighbors**

Establishes BFD sessions with all neighbors of the corresponding interface which are greater than or equal to “2-way” state.

```
ipv6 ospf interface if_name bfd-state all-neighbors {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>if_name</td>
<td>The name of an existing OSPFv3 interface.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables BFD sessions with all neighbors.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD sessions with all neighbors.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The specified OSPFv3 interface must be enabled to interact with BFD.
- The BFD status for OSPFv3 must be enabled before OSPFv3 can interact with BFD.

**Examples**

```
-> ipv6 ospf interface int1 bfd-state all-neighbors enable
-> ipv6 ospf interface int1 bfd-state all-neighbors disable
```

**Release History**

Release 8.4.1.R03; command was introduced.
**Related Commands**

- `ipv6 ospf bfd-state`  Enables or disables the BFD status for OSPFv3 protocol.
- `ipv6 ospf bfd-state all-interfaces`  Enables or disables BFD for all OSPFv3 interfaces configured.
- `ipv6 ospf interface bfd-state`  Enables or disables BFD for a specific OSPFv3 interface.
- `ipv6 ospf interface bfd-state drs-only`  Establishes BFD sessions only on neighbors in full state.
- `show ipv6 ospf interface`  Displays configuration information for an OSPFv3 interface.

**MIB Objects**

- `alaOspf3IfAugTable`
- `alaOspf3IfDrsOnly`
**show ipv6 ospf**

Displays the OSPFv3 status and general configuration parameters.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used to display the general configuration parameters of the OSPFv3 router. See the Related Commands section below for commands that are used to modify the displayed parameters.

**Examples**

```plaintext
-> show ipv6 ospf
Status = Enabled,
Router ID = 30.1.1.2,
# Areas = 1,
# Interfaces = 3,
Area Border Router = No,
AS Border Router = No,
External Route Tag = 0,
SPF Hold (seconds) = 10,
SPF Delay (seconds) = 5,
MTU checking = Enabled,
BFD Status = Disabled,
# SPF calculations performed = 34,
Last SPF run (seconds ago) = N/A,
# of routes = 1,
# of AS external LSAs = 0,
# of neighbors that are in:
  Full state = 1,
  Loading state = 0,
  Exchange state = 0,
  Exstart state = 0,
  2way state = 0,
```
Init state = 0,
Attempt state = 0,
Down state = 0,
Restart Support = Enabled,
Restart Status = Restating,
Restart Helper Support = Enabled,
Restart Helper Status = NotHelping

output definitions

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays whether OSPFv3 is currently enabled or disabled on the router.</td>
</tr>
<tr>
<td>Router Id</td>
<td>The unique identification for the router.</td>
</tr>
<tr>
<td># Areas</td>
<td>Number of areas to which the router belongs.</td>
</tr>
<tr>
<td># Interface</td>
<td>Number of interfaces participating in OSPFv3.</td>
</tr>
<tr>
<td>Area Border Router</td>
<td>Displays whether the router status is an area router or not.</td>
</tr>
<tr>
<td>AS Border Router</td>
<td>Displays whether the area Autonomous System Border Router status of this router is enabled or disabled.</td>
</tr>
<tr>
<td>External Route Tag</td>
<td>Displays the route tag for this router.</td>
</tr>
<tr>
<td>SPF Hold (seconds)</td>
<td>Displays the time in seconds between the reception of an OSPFv3 topology change and the start of a SPF calculation.</td>
</tr>
<tr>
<td>SPF Delay (seconds)</td>
<td>Displays the time in seconds between consecutive SPF calculations.</td>
</tr>
<tr>
<td>MTU Checking</td>
<td>Displays whether Maximum Transfer Unit checking is enabled or disabled.</td>
</tr>
<tr>
<td>BFD Status</td>
<td>Displays whether BFD monitoring is enabled or disabled for OSPF.</td>
</tr>
<tr>
<td># SPF calculations performed</td>
<td>Displays the number of SPF calculation performed.</td>
</tr>
<tr>
<td>Last SPF run (seconds ago)</td>
<td>N/A</td>
</tr>
<tr>
<td># of routes</td>
<td>The total number of OSPFv3 routes known to this router.</td>
</tr>
<tr>
<td># of AS external LSAs</td>
<td>The number of external routes learned from outside the router’s Autonomous System (AS).</td>
</tr>
</tbody>
</table>

# of neighbors that are in:

| Full state          | Displays the number of neighbor routers that are in Full state.            |
| Loading state       | Displays the number of neighbor routers that are in Loading state.         |
| Exchange state      | Displays the number of neighbor routers that are in Exchange state.        |
| Exstart state       | Displays the number of neighbor routers that are in Exstart state.         |
| 2way state          | Displays the number of neighbor routers that are in 2way state.            |
| Init state          | Displays the number of neighbor routers that are in Init state.            |
| Attempt state       | Displays the number of neighbor routers that are in Attempt state.         |
| Down state          | Displays the number of neighbor routers that are in Down state.            |
| Restart Support     | Indicates if graceful restart feature is enabled or disabled on an OSPFv3 router. |
| Restart Status      | Displays the OSPFv3 graceful restart status.                               |
| Restart Helper Support | Indicates whether the router is acting as a restart helper for the neighbor. |
| Restart Helper Status | Displays the OSPFv3 graceful restart helper status.                        |
**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1: OSPFv3 graceful restart fields added.

**Related Commands**

- `ipv6 ospf admin-state` Enables or disables the administration of OSPFv3 on the router.
- `ip router router-id` Configures the router ID for the router.
- `ipv6 ospf route-tag` Configures a tag value for Autonomous System External (ASE) routes created.
- `ipv6 ospf spf-timer` Configures timers for SPF calculation.
- `ipv6 ospf mtu-checking` Enables or disables the use of Maximum Transfer Unit (MTU) checking.
- `ipv6 ospf bfd-state` Enables or disables the registration of OSPFv3 with the BFD protocol.
- `ipv6 ospf restart` Configures graceful restart feature on an OSPFv3 router.
- `ipv6 ospf restart-helper` Enables the graceful restart helper functionality.

**MIB Objects**

- `ospfv3GeneralGroup`
  - `ospfv3RouterId`
  - `ospfv3AdminStat`
  - `ospfv3VersionNumber`
  - `ospfv3AreaBdrRtrStatus`
  - `ospfv3ASBdrRtrStatus`
  - `ospfv3OriginateNewLsas`
  - `ospfv3RxNewLsas`
  - `ospfv3ExitOverflowInterval`
- `alaProtocolOspf3`
  - `alaOspf3RedistAdminStatus`
  - `alaOspf3RedistRouteTag`
  - `alaOspf3TimerSpfDelay`
  - `alaOspf3TimerSpfHold`
  - `alaOspf3MtuCheck`
  - `alaOspf3BfdStatus`
  - `ospfv3RestartSupport`
  - `ospfv3RestartStatus`
  - `alaOspf3RestartHelperSupport`
  - `alaOspf3RestartHelperStatus`
show ipv6 ospf border-routers

Displays information regarding all or specified border routers.

show ipv6 ospf border-routers [area area_id] [router router_id]

Syntax Definitions

area_id A unique 32-bit value in IP address format.

router_id A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is used to display a list of border routers known by this OSPFv3 router.

- By using the optional parameters, you can display the border routers using the specified parameter. For example, to find a router using a router ID of 1.1.1.1, enter the command using the router ID of 1.1.1.1 as a search criteria.

- See the Related Commands sections below to modify the list.

Examples

-> show ipv6 ospf border-routers

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Area</th>
<th>Metric</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.6.6</td>
<td>0.0.0.0</td>
<td>2</td>
<td>INTRA</td>
</tr>
<tr>
<td>6.6.6.6</td>
<td>0.0.0.1</td>
<td>2</td>
<td>INTRA</td>
</tr>
<tr>
<td>fe80::2d0:95ff:fee2:6bda -&gt; pseudo1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fe80::2d0:95ff:fee2:6bda -&gt; pseudo2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

output definitions

- **Router ID**: The unique identification for the router.
- **Area**: A unique 32-bit value, such as an IP address, that identifies a neighboring router in the Autonomous System.
output definitions (continued)

<table>
<thead>
<tr>
<th>Metric</th>
<th>The metric used by the routes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The type of routes specified (intra or inter).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**show ipv6 ospf**

Displays the OSPFv3 status and general configuration parameters.

**MIB Objects**

N/A
**show ipv6 ospf host**

Displays information on the configured OSPFv3 hosts.

```
show ipv6 ospf host [ipv6_address]
```

### Syntax Definitions

`ipv6_address`  
A 128-bit IP address for a directly attached host.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is used to display general information for OSPFv3 hosts directly attached to this router.
- See the Related Commands section below to modify the list.

### Examples

```
-> show ipv6 ospf host

Area     Metric Address
----------+-----------+-----------
0.0.0.1   1  2001::1/64
```

**output definitions**

- **Area**: A 32-bit IP address for a directly attached host. This can be set using the `ipv6 ospf host` command.
- **Metric**: The metric assigned to the host. Metric is set using the `ipv6 ospf host` command.
- **Address**: IPv6 address of the host.

### Release History

Release 7.1.1; command was introduced.
Related Commands

**ipv6 ospf host**   Creates or deletes an OSPFv3 entry for directly attached hosts.

MIB Objects

ospfv3HostTable
  ospfv3HostIpAddress
  ospfv3HostMetric
  ospfHostStatus
  ospfv3HostAreaID
**show ipv6 ospf lsdb**

Displays Link State Advertisements (LSAs) in the Link State Database (LSDB) associated with each area.

```
show ipv6 ospf lsdb [area area_id] [rtr | net | netsum | asbrsum] [linkstate-id ls_id] [router-id router_id]
```

**Syntax Definitions**

- `area_id`: A unique 32-bit value in IP address format.
- `rtr`: Specifies router LSAs.
- `net`: Specifies network LSAs.
- `netsum`: Specifies network summary LSAs.
- `asbrsum`: Specifies Autonomous System Border Router summary LSAs.
- `ls_id`: The Link state ID. The ID is a unique 32-bit value, such as an IP address. This number is used as a record in the link state database.
- `router_id`: The Router ID. The ID is a unique 32-bit value such as an IP address.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is used to display the LSDB of the OSPFv3 router. It can be used for OSPFv3 debugging, specifically to narrow down sections of an area to determine which sections are receiving the specified LSAs. You can specify the parameters of only the area LSDB using the optional command parameters.
- You can view LSAs by specifying either a link state identifier or a router identifier. However, when specifying a router ID, you also need to supply a valid link state ID.

**Examples**

```
-> show ipv6 ospf lsdb
```

<table>
<thead>
<tr>
<th>Area</th>
<th>Type</th>
<th>Link ID</th>
<th>Advertising Rtr</th>
<th>Sequence #</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>0</td>
<td>1.1.1.1</td>
<td>8000020f</td>
<td>1117</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>0</td>
<td>3.3.3.3</td>
<td>80000208</td>
<td>1121</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>The identification of the area to which the router belongs.</td>
</tr>
<tr>
<td>Type</td>
<td>The protocol type from where the route was learned.</td>
</tr>
<tr>
<td>Link Id</td>
<td>The Link state ID. The ID is a unique 32-bit value expressed as an IPv6 address. This number is used as a record in the link state database.</td>
</tr>
<tr>
<td>Advertising Rtr</td>
<td>The ID of the router that advertises the routes.</td>
</tr>
<tr>
<td>Sequence #</td>
<td>The advertisement sequence number (i.e., a value used to identify old and duplicate link state advertisements).</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the LSA in seconds. That is, the duration for which this entry has existed in the external database.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ipv6 ospf admin-state** Displays the OSPFv3 status and general configuration parameters.

**MIB Objects**

- `ospfv3AsLsdbTable`  
  - `ospfv3AsLsdbAreaId`  
  - `ospfv3AsLsdbType`  
  - `ospfv3AsLsdbLsid`  
  - `ospfv3AsLsdbRouterId`  
  - `ospfv3AsLsdbAdvertisement`  
  - `ospfv3AsLsdbSequence`  
  - `ospfv3AsLsdbAge`
show ipv6 ospf neighbor

Displays information on OSPFv3 non-virtual neighbors.

show ipv6 ospf neighbor [router ipv4_address][interface interface_name]

**Syntax Definitions**

- `ipv4_address`: A 32-bit router ID of the neighboring router.
- `interface_name`: The name of the interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is used to display all non-virtual neighbors of the OSPFv3 router.
- See the Related Commands section below to modify the list.

**Examples**

```
-> show ipv6 ospf neighbor
Router ID          Area/Transit Area  State  Interface
----------------+--------------------+-----+----------------------------------
1.1.1.1           0.0.0.0              FULL  vlan-2071
3.3.3.3           0.0.0.0              FULL  vlan-2071
5.5.5.5           0.0.0.0              FULL  vlan-2071
23.23.23.23       0.0.0.1              FULL  vlan-2055
23.23.23.23       0.0.0.1              FULL  vlan-2056
24.24.24.24       0.0.0.1              FULL  vlan-2065
24.24.24.24       0.0.0.1              FULL  vlan-2066
```

**output definitions**

- **Router ID**: The unique identification for the router.
- **Area/Transit Area**: The area identifier.
- **State**: The state of the OSPFv3 neighbor adjacency.
- **Interface**: The name of the interface.
-> show ipv6 ospf neighbor router 24.24.24.24

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Area/Transit Area</th>
<th>State</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>24.24.24.24</td>
<td>0.0.0.1</td>
<td>FULL</td>
<td>vlan-2070</td>
</tr>
<tr>
<td>24.24.24.24</td>
<td>0.0.0.1</td>
<td>FULL</td>
<td>vlan-2073</td>
</tr>
</tbody>
</table>

**output definitions**

**Router ID**
The unique identification for the router.

**Area/Transit Area**
The area identifier.

**State**
The state of the OSPFv3 neighbor adjacency.

**Interface**
The name of the interface.

-> show ipv6 ospf neighbor router 1.1.1.1 interface v14

Details for Neighbor 1.1.1.1

<table>
<thead>
<tr>
<th>State</th>
<th>FULL,</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Dynamic,</td>
</tr>
<tr>
<td>Interface</td>
<td>v14,</td>
</tr>
<tr>
<td>Neighbor i/f index</td>
<td>21,</td>
</tr>
<tr>
<td>Priority</td>
<td>1,</td>
</tr>
<tr>
<td>Address</td>
<td>fe80::eae7:32ff:e71:cc69,</td>
</tr>
<tr>
<td>Neighbor is reporting DR as</td>
<td>30.1.1.2,</td>
</tr>
<tr>
<td>Neighbor is reporting BDR as</td>
<td>1.1.1.1,</td>
</tr>
<tr>
<td>Neighbor is Master/Slave</td>
<td>Master,</td>
</tr>
<tr>
<td>Seconds since last Hello seen</td>
<td>8,</td>
</tr>
<tr>
<td># of LSAs on retransmit list</td>
<td>0,</td>
</tr>
<tr>
<td># of LSAs on request list</td>
<td>0,</td>
</tr>
<tr>
<td># of State Changes</td>
<td>6,</td>
</tr>
<tr>
<td>Restart Helper Status</td>
<td>NotHelping,</td>
</tr>
<tr>
<td>Restart Age</td>
<td>0 sec,</td>
</tr>
<tr>
<td>Last Restart Helper Exit Reason</td>
<td>None</td>
</tr>
</tbody>
</table>

**Neighbor options:**

V6 bit is set
E bit is set
MC bit is not set
N bit is not set
R bit is set
DC bit is not set

**output definitions**

**State**
The state of the OSPFv3 neighbor adjacency.

**Type**
Specifies the type of neighbor.

**Interface**
The name of the interface.

**Neighbor i/f index**
The unique value assigned to the neighbor.

**Priority**
The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.

**Address**
The IPv6 address of the host.

**Neighbor is reporting DR as**
The address of the neighbors designated router.

**Neighbor is reporting BDR as**
The address of the neighbors Backup Designated Router.

**Neighbor is Master/Slave**
The role the neighbor has with the local router during DD Exchange, which can be Master or Slave.
### Output Definitions (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds since last Hello seen</td>
<td>The amount of time (in seconds) since the last HELLO messages was received from this neighbor.</td>
</tr>
<tr>
<td># of LSAs on retransmit list</td>
<td>The number of Link State updates to the neighbor that need to be retransmitted by the OSPFv3 router.</td>
</tr>
<tr>
<td># of LSAs on request list</td>
<td>The number of Link State requests to this neighbor that have not received a response from this neighbor.</td>
</tr>
<tr>
<td># of State Changes</td>
<td>The number of times this OSPFv3 interface has changed its state.</td>
</tr>
<tr>
<td>Restart Helper Status</td>
<td>Indicates whether the router is acting as a restart helper for the neighbor.</td>
</tr>
<tr>
<td>Restart Age</td>
<td>The remaining time, in seconds, for the current OSPFv3 restart interval if the router is acting as a restart helper for the neighbor.</td>
</tr>
<tr>
<td>Last Restart Helper Exit Reason</td>
<td>The outcome of the last attempt at acting as a restart helper for the neighbor.</td>
</tr>
<tr>
<td>Neighbor options</td>
<td>If set:</td>
</tr>
<tr>
<td>V6 - V6 support</td>
<td></td>
</tr>
<tr>
<td>R - If clear, a node can participate in OSPFv3 topology distribution without being used to forward transit traffic</td>
<td></td>
</tr>
<tr>
<td>N - Type 7 LSA support</td>
<td></td>
</tr>
<tr>
<td>MC - Multicast support</td>
<td></td>
</tr>
<tr>
<td>E - External routes support</td>
<td></td>
</tr>
<tr>
<td>DC - Demand circuit support</td>
<td></td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1: command was introduced.
Release 8.4.1: OSPFv3 graceful restart fields added.

### Related Commands

**show ipv6 ospf**

Displays the OSPFv3 status and general configuration parameters.

### MIB Objects

- `ospfv3NbrTable`
  - `ospfv3NbrAddress`
  - `ospfv3NbrRtrId`
  - `ospfv3NbrOptions`
  - `ospfv3NbrPriority`
  - `ospfv3NbrState`
  - `ospfv3NbrEvents`
  - `ospfv3NbrHelloSuppressed`
  - `ospfv3NbrRestartHelperStatus`
  - `ospfv3NbrRestartHelperAge`
  - `ospfv3NbrRestartHelperExitReason`
  - `ospfv3VirtNbrRestartHelperStatus`
  - `ospfv3VirtNbrRestartHelperAge`
  - `ospfv3VirtNbrRestartHelperExitReason`
show ipv6 ospf routes

Displays the OSPFv3 routes known to the router.

**show ipv6 ospf routes [prefix ipv6_address_prefix][gateway gateway]**

### Syntax Definitions

- **ipv6_address_prefix**
  The 128-bit IPv6 address of the route destination in hexadecimal format.
- **gateway**
  The next hop IPv6 address for this router.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td>X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If no variables are entered, all routes are displayed.
- If the variables are entered, then only routes matching the specified criteria are shown.
- All the variables described above must be entered for a route match. If all of the variables are not entered, an error message is returned.

### Examples

```
-> show ipv6 ospf routes

Prefix                             Path Type  Metric
                                      1 : 2
::/0                                INTER       2 : -
   fe80::2d0:95ff:fee0:710c -> vlan-2071
2051::/64                            INTRA       2 : -
   fe80::2d0:95ff:feac:a59f -> vlan-2055
   fe80::2d0:95ff:feac:a59f -> vlan-2056
   fe80::2d0:95ff:fed7:747e -> vlan-2065
   fe80::2d0:95ff:fed7:747e -> vlan-2066
```

### output definitions

- **Prefix**
  The destination address of the IPv6 route in the hexadecimal format.
output definitions

| Path Type | The type of routes specified (intra or inter). |
| Metric    | The cost of the route.                        |

Release History

Release 7.1.1; command was introduced.

Related Commands

ipv6 ospf admin-state Displays the OSPFv3 status and general configuration parameters.

MIB Objects

N/A
show ipv6 ospf virtual-link

Displays virtual link information. A virtual link is used to connect OSPFv3 backbone routers that are not physically contiguous.

show ipv6 ospf virtual-link [router_id]

Syntax Definitions

router_id

The router ID of the remote end of the virtual link.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 ospf virtual-link

Transit Area Peer Router ID Intf Nbr
-----------------------------------------------
0.0.0.1 6.6.6.6 P2P  FULL 2

output definitions

Transit Area The area identification for the area assigned to the virtual link.
Peer Router ID The destination router identification for the virtual link.
Intf State The state of the virtual link with regards to the local router.
Nbr State The state of the virtual link adjacency.
Cost The cost metric of the route.

Release History

Release 7.1.1; command was introduced.
**Related Commands**

`ipv6 ospf virtual-link`  
Creates or deletes a virtual link.

**MIB Objects**

`ospfv3VirtIfTable`
- `ospfv3VirtIfAreaId`
- `ospfv3VirtIfNeighbor`
- `ospfv3VirtIfState`
show ipv6 ospf area

Displays either all OSPFv3 areas, or a specified OSPFv3 area.

show ipv6 ospf area [area_id]

Syntax Definitions

area_id A unique 32-bit value in IP address format.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Allows you to view the details of a specified OSPFv3 area.
- If an OSPFv3 area is not specified, all known areas for the OSPFv3 router will be displayed.
- See the Related Commands section below for information on modifying an area.

Examples

-> show ipv6 ospf area

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Type</th>
<th>Metric</th>
<th>Number of Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Normal</td>
<td>NA</td>
<td>2</td>
</tr>
<tr>
<td>0.0.0.1</td>
<td>Stub</td>
<td>1000000</td>
<td>2</td>
</tr>
<tr>
<td>0.0.0.2</td>
<td>Nssa</td>
<td>1000</td>
<td>1</td>
</tr>
</tbody>
</table>

-> show ipv6 ospf area 0.0.0.0

Details for Area 0.0.0.0

Area Type = Normal,
Area Stub Metric = 0,
# of SPF calculations = 0,
# Interfaces = 2,
# Router LSAs = 0,
# Network LSAs = 0,
# Intra-area-prefix LSAs = 0,
# Inter-area-prefix LSAs = 0,
# Inter-area-router LSAs = 0,
# hosts = 0,
# ABRs = 0,
# ASBRs = 0,
Summarization ranges = 0

-> show ipv6 ospf area 0.0.0.1
Details for Area 0.0.0.1

Area Type = Stub,
Area Stub Metric = 1000000,
# of SPF calculations = 2,
# Interfaces = 2,
# Router LSAs = 0,
# Network LSAs = 0,
# Intra-area-prefix LSAs = 0,
# Inter-area-prefix LSAs = 0,
# Inter-area-router LSAs = 0,
# hosts = 0,
# ABRs = 0,
# ASBRs = 0,
Summarization ranges = 2
  Range #0, address 2001::/64, filter no
  Range #1, address 2002::/64, filter yes
Import Area Summaries = Enabled

-> show ipv6 ospf area 0.0.0.2
Details for Area 0.0.0.2

Area Type = NSSA,
Area Stub Metric = 1000,
# of SPF calculations = 2,
# Interfaces = 1,
# Router LSAs = 3,
# Network LSAs = 2,
# Intra-area-prefix LSAs = 2,
# Inter-area-prefix LSAs = 1,
# Inter-area-router LSAs = 0,
# hosts = 0,
# ABRs = 1,
# ASBRs = 2,
Summarization ranges = 0
Import Area Summaries = Enabled
NSSA Translator Role = Candidate
NSSA Translator State = Elected
# NSSA Translator State Changes = 1,

**output definitions**

**Area Type**
The area type. This field will be normal, stub, or NSSA.

**Area Stub Metric**
Indicates whether the area is enabled or disabled.

**# Router LSAs**
The total number of Link State Advertisements for the Area.

**# Network LSAs**
The total number of inter-area Link State Advertisements.

**# of SPF calculations**
The number of times the area has calculated the Shortest Path.

**# Interfaces**
The number of OSPFv3 interfaces.

**# Intra-area-prefix LSAs**
The number of intra-area-prefix LSAs, which associates a list of IPv6 address prefixes with a router by referencing a router-LSA.
output definitions (continued)

<table>
<thead>
<tr>
<th># Inter-area-prefix LSAs</th>
<th>The number of inter-area-prefix LSAs. Corresponds to Type 3 summary-LSA of OSPFv3.</th>
</tr>
</thead>
<tbody>
<tr>
<td># Inter-area-router LSAs</td>
<td>The number of inter-area-router LSAs. Corresponds to Type 4 summary-LSA of OSPFv3.</td>
</tr>
<tr>
<td># hosts</td>
<td>The number of directly attached hosts.</td>
</tr>
<tr>
<td># ABRs</td>
<td>Number of Area Border Routers in the area.</td>
</tr>
<tr>
<td># ASBRs</td>
<td>Number of Autonomous System Border Routers in the area.</td>
</tr>
<tr>
<td>Summarization ranges</td>
<td>The range of prefixes summarized in to the area.</td>
</tr>
<tr>
<td>Import Area Summaries</td>
<td>Specifies whether or not summary routes are imported into the stub or NSSA as Type-3 summary-LSAs.</td>
</tr>
<tr>
<td>NSSA Translator Role</td>
<td>Specifies the NSSA translator role: Candidate or Always</td>
</tr>
<tr>
<td>NSSA Translator State</td>
<td>Indicates if and how an NSSA border router is performing NSSA translation (<strong>ipv6 ospf area nssa-translator-role</strong>) of NSSA-LSAs into AS-External-LSAs: Enabled, Elected, Disabled. <strong>Enabled</strong> indicates that the NSSA border router's translator role has been set to 'always'. <strong>Elected</strong> indicates that a candidate NSSA border router is translating NSSA-LSAs into AS-External-LSAs. <strong>Disabled</strong> indicates that a candidate NSSA Border router is not translating NSSA-LSAs into AS-External-LSAs.</td>
</tr>
<tr>
<td># NSSA Translator State</td>
<td>Indicates the number of translator state changes that have occurred since the last start-up of the OSPFv3 routing process.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; NSSA related fields added.

Related Commands

- **ipv6 ospf area**  Creates or deletes an OSPFv3 area, assigning default metric, cost, and type.
- **show ipv6 ospf interface**  Displays OSPFv3 interface information.

MIB Objects

- ospfv3AreaTable
  - ospfv3AreaId
  - ospfv3ImportAsExtern
  - ospfv3SpfRuns
  - ospfv3AreaBdrRtrCount
  - ospfv3AreaSummary
  - ospfv3AreaStatus
  - ospfv3AreaNssaTranslatorRole
  - ospfv3AreaNssaTranslatorState
  - ospfv3AreaNssaTranslatorStabInterval
  - ospfv3AreaNssaTranslatorEvents
show ipv6 ospf interface

Displays OSPFv3 interface information.

show ipv6 ospf interface [interface_name]

Syntax Definitions

interface_name: The name of the interface.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform Code</th>
<th>Supported Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6360, 6465, 6560, 6570M, 6860, 6860N, 6865, 6900, 6900, 6900 V72/C32, 6900 X48C6/T48C6, X48C4E/V48C8, C32E/T24C2, X24C2</td>
</tr>
</tbody>
</table>

Usage Guidelines

Not specifying the interface name displays all known interfaces for the OSPFv3 router.

Examples

```
-> show ipv6 ospf interface
```

output definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>DR Router ID</th>
<th>BDR Router ID</th>
<th>IPv6 Intf Status</th>
<th>IPv6 Intf Type</th>
<th>IPv6 Intf State</th>
<th>IPv6 BFD Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-2071</td>
<td>5.5.5.5</td>
<td>0.0.0.0</td>
<td>Enabled</td>
<td>BCAST</td>
<td>DR</td>
<td>Enabled</td>
</tr>
<tr>
<td>vlan-2055</td>
<td>7.7.7.7</td>
<td>5.5.5.5</td>
<td>Enabled</td>
<td>BCAST</td>
<td>BDR</td>
<td>Enabled</td>
</tr>
<tr>
<td>vlan-2056</td>
<td>7.7.7.7</td>
<td>5.5.5.5</td>
<td>Enabled</td>
<td>BCAST</td>
<td>BDR</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

Name: The name of the interface.
DR Router ID: The designated router address on this network segment. Make sure you configure a VLAN for the router IP. (See Chapter 5, “VLAN Management Commands,” for more information.)
BDR Router ID: The IP address of the backup designated router.
Admin Status: The current administration status of the interface, either enabled or disabled.
IPv6 Intf Status: Indicates whether the interface is an active OSPFv3 interface.
Intf Type: Whether the interface is assigned to a VLAN or tunnel.
-> show ipv6 ospf interface vlan-2071
Details for Intf 'vlan-2071'

Name                             = vlan-2071,
Type                             = BROADCAST,
Admin Status                     = Enabled,
IPv6 Interface Status            = Up,
Oper Status                      = Up,
State                            = DR,
Area                             = 0.0.0.0,
Priority                         = 100,
Cost                             = 1,
Designated Router                = 3.3.3.3,
Backup Designated Router         = 0.0.0.0,
Hello Interval                   = 1,
Router Dead Interval             = 4,
Retransmit Interval              = 5,
Transit Delay                    = 1,
Ifindex                          = 17
IPv6 'ifindex'                   = 2071,
MTU                              = 1500,
Link LSA suppression             = disabled,
BFD Status                       = disabled,
# of attached neighbors          = 0,
# of state changes               = 0,
Link-local address               = fe80::2efa:a2ff:fe13:e402

Output fields when an IP address or interface name is specified are described below:

output definitions (continued)

<table>
<thead>
<tr>
<th>Intf State</th>
<th>The current state of the OSPFv3 interface. It will be DR, BDR, other.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Status</td>
<td>The current status of BFD for the OSPFv3 interface.</td>
</tr>
</tbody>
</table>

Type
The OSPFv3 interface type, which can be Broadcast, NBMA, Point-to-Point, or Point-to-Multipoint.

Admin Status
The current administrative status of the interface, either enabled or disabled.

IPv6 Interface Status
The current administrative status of the IPv6 interface, either up or down.

Oper Status
Indicates whether the interface is an active OSPFv3 interface.

State
The current state of the OSPFv3 interface. It will be down, up, dp, dr, or other.

Area
The area identification number to which the interface is assigned. This field is not applicable if an interface has not yet been assigned to an area.

Priority
The priority of the interface with regards to becoming the designated router. The higher the number, the higher the priority.

Cost
The cost added to routes learned on this interface.

Designated Router
The identification number of the designated router.

Backup Designated Router
The identification number of the backup designated router.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello Interval</td>
<td>The number of seconds between hello messages sent out on the interface.</td>
</tr>
<tr>
<td>Router Dead Interval</td>
<td>The number of seconds the interface waits for hello messages received from</td>
</tr>
<tr>
<td></td>
<td>a neighbor before declaring the neighbor as dead.</td>
</tr>
<tr>
<td>Retransmit Interval</td>
<td>The number of seconds the interface waits before resending hello messages.</td>
</tr>
<tr>
<td>Transit Delay</td>
<td>The estimated number of seconds required to transmit a link state update</td>
</tr>
<tr>
<td></td>
<td>over this interface.</td>
</tr>
<tr>
<td>Ifindex</td>
<td>The unique value assigned to an interface.</td>
</tr>
<tr>
<td>IPv6 ‘ifindex’</td>
<td>The unique value assigned to an IPv6 interface.</td>
</tr>
<tr>
<td>MTU</td>
<td>The Maximum Transfer Unit (in bytes) for the interface.</td>
</tr>
<tr>
<td>Link LSA suppression</td>
<td>Whether or not (enabled or disabled) link LSA origination is</td>
</tr>
<tr>
<td></td>
<td>suppressed for broadcast or NBMA interface types.</td>
</tr>
<tr>
<td>BFD Status</td>
<td>The status of BFD on this interface.</td>
</tr>
<tr>
<td># of attached neighbors</td>
<td>The number of OSPFv3 neighbors in the initialization state.</td>
</tr>
<tr>
<td># of state changes</td>
<td>The number of times this OSPFv3 interface has changed its state.</td>
</tr>
<tr>
<td>Link-local address</td>
<td>A globally unique IPv6 address.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R03; **bfd status** field added.

**Related Commands**

- `ipv6 ospf interface` Creates and deletes an OSPFv3 interface.
- `ipv6 ospf interface dead-interval` Configures the OSPFv3 interface dead interval.
- `ipv6 ospf interface hello-interval` Configures the OSPFv3 interface hello interval.
- `ipv6 ospf interface cost` Configures the OSPFv3 interface cost.
- `ipv6 ospf interface priority` Configures the OSPFv3 interface priority.
- `ipv6 ospf interface retrans-interval` Configures the OSPFv3 interface retransmit interval.
- `ipv6 ospf interface transit-delay` Configures the OSPFv3 interface transit delay.
- `ipv6 ospf interface area` Configures an OSPFv3 interface area.
- `ipv6 ospf interface admin-state` Enables or disables the administration status on an OSPFv3 interface.
- `ipv6 ospf interface suppress-link-lsa` Configures whether or not link LSA origination is suppressed for broadcast or NBMA interface types.
- `ipv6 ospf interface bfd-state` Enables or disables the status of BFD for an OSPFv3 interface.
**MIB Objects**

ospfv3IfTable
  ospfv3IfAreaId
  ospfv3IfType
  ospfv3IfAdminStat
  ospfv3IfRtrPriority
  ospfv3IfTransitDelay
  ospfv3IfRetransInterval
  ospfv3IfHelloInterval
  ospfv3IfRtrDeadInterval
  ospfv3IfPollInterval
  ospfv3IfState
  ospfv3IfDesignatedRouter
  ospfv3IfBackupDesignatedRouter
  ospfv3IfEvents
  ospfv3IfStatus
  ospfv3IfLinkLSASuppression

alaOspf3IfAugTable
  alaOspf3IfBfdStatus
**ipv6 ospf restart**

Configures graceful restart feature on an OSPFv3 router.

`ipv6 ospf restart`

---

**Syntax Definitions**

N/A

**Defaults**

Graceful restart is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6 X48C4E/V48C8 C32E/T24C2 X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to disable support for the graceful restart feature on an OSPFv3 router.

- The minimum hardware configuration for this command is a dual CMM configuration. The chassis based products (OmniSwitch 9900) running in a standalone or VC-1 mode must have dual CMMs. Stackable switches (such as the OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900) or chassis based switches running with single CMM must have two or more chassis in the VC.

- This command enables both planned and unplanned restarts.

**Examples**

```
-> ipv6 ospf restart
-> no ipv6 ospf restart
```

**Release History**

Release 8.4.1; command introduced
**Related Commands**

- **show ipv6 ospf restart** Displays the OSPFv3 graceful restart related configuration and status.
- **show ipv6 ospf** Displays the OSPFv3 status and general configuration parameters.
- **show ipv6 ospf neighbor** Displays information on OSPFv3 non-virtual neighbors.

**MIB Objects**

- ospfv3RestartSupport
- ospfv3RestartStatus
- ospfv3RestartAge
- ospfv3RestartExitReason
- ospfv3RestartTime
ipv6 ospf restart initiate

Initiates a planned OSPFv3 graceful restart.

ipv6 ospf restart initiate

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command must be executed before executing the `takeover` or `vctakeover` command.

Example

-> ipv6 ospf restart initiate

Release History

Release 8.4.1; command introduced

Related Commands

show ipv6 ospf restart

Displays the OSPFv3 graceful restart related configuration and status.

MIB Objects

alaOspf3RestartInitiate
**ipv6 ospf restart interval**

Configures the grace period for achieving a graceful OSPFv3 restart.

**ipv6 ospf restart interval [seconds]**

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Restart timeout interval. The valid range is 1–1800 seconds.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>120</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Restart interval must be configured based on the databases size, number of neighbors, and number of OSPFv3 areas of the restarting router. If this is configured too low, there is a chance that graceful restart may fail prematurely.

**Example**

```
-> ipv6 ospf restart interval 180
-> no ipv6 ospf restart interval
```

**Release History**

Release 8.4.1; command introduced
Related Commands

- **ipv6 ospf restart**
  - Configures graceful restart feature on an OSPFv3 router.

- **show ipv6 ospf restart**
  - Displays the OSPFv3 graceful restart related configuration and status.

MIB Objects

- **ospfv3RestartInterval**
**ipv6 ospf restart-helper**

Enables the graceful restart helper functionality.

**ipv6 ospf restart-helper**

---

**Syntax Definitions**

N/A

**Defaults**

By default, graceful restart helper functionality is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to disable restart helper functionality.
- A router that has configured as a helper may reject helping or stop helping in the half way if there is any topology change in the OSPFv3 network.
- The graceful restart helper does not have a requirement of having dual CMMs.

**Examples**

- `ipv6 ospf restart-helper`
- `no ipv6 ospf restart-helper`

**Release History**

Release 8.4.1; command introduced
**Related Commands**

- `ipv6 ospf restart` Configures graceful restart feature on an OSPFv3 router.
- `ipv6 ospf restart-helper strict-lsa-check` Administratively enables and disables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.
- `show ipv6 ospf restart` Displays the OSPFv3 graceful restart related configuration and status.

**MIB Objects**

- `alaOspf3RestartHelperSupport`
- `alaOspf3RestartHelperStatus`
- `ospfv3NbrRestartHelperStatus`
- `ospfv3NbrRestartHelperAge`
- `ospfv3NbrRestartHelperExitReason`
- `ospfv3VirtNbrRestartHelperStatus`
- `ospfv3VirtNbrRestartHelperAge`
- `ospfv3VirtNbrRestartHelperExitReason`
**ipv6 ospf restart-helper strict-lsa-check**

Enables whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

**IPv6 ospf restart-helper strict-lsa-check**

**Syntax Definitions**

N/A

**Defaults**

By default, strict-lsa-checking is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the no form of the command to disable this functionality.
- Disabling this functionality may create sub-optimal or black hole routes during the graceful restart period.
- This functionality does not have a requirement of having dual CMMs.

**Examples**

- `-> ipv6 ospf restart-helper strict-lsa-check`
- `-> no ipv6 ospf restart-helper strict-lsa-check`

**Release History**

Release 8.4.1; command introduced
Related Commands

- **ipv6 ospf restart**: Configures graceful restart feature on an OSPFv3 router.
- **ipv6 ospf restart-helper**: Administratively enables the capability of an OSPFv3 router to operate in helper mode in response to a router performing a graceful restart.
- **show ipv6 ospf restart**: Displays the OSPFv3 graceful restart related configuration and status.

MIB Objects

- **ospfv3RestartStrictLsaChecking**
**show ipv6 ospf restart**

Displays the OSPFv3 graceful restart related configuration and status.

```plaintext
-> show ipv6 ospf restart
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```plaintext
-> show ipv6 ospf restart
Restart Support = Enabled (planned-unplanned),
Restart Status = Not Restarting,
Restart Interval = 120,
Restart Age = 0,
Last Restart Exit Reason = None,
Restart Helper Support = Enabled,
Restart Helper Strict Checking = Enabled,
Restart Helper Status = NotHelping,
Time Since Exit Reason Updated = 21:09:58
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart Support</td>
<td>The administrative status of OSPFv3 graceful restart.</td>
</tr>
<tr>
<td>Restart Status</td>
<td>The current status of OSPFv3 graceful restart, which can be <strong>Not Restarting</strong>, <strong>Unplanned Restart</strong> (after a CMM takeover), or <strong>Planned Restart</strong> (before CMM takeover).</td>
</tr>
<tr>
<td>Restart Interval</td>
<td>The configured OSPFv3 restart timeout interval, in seconds.</td>
</tr>
<tr>
<td>Restart Age</td>
<td>The remaining time, in seconds, for the current OSPFv3 graceful restart interval.</td>
</tr>
</tbody>
</table>
**OSPFv3 Commands**

**show ipv6 ospf restart**

---

**Last Restart Exit Reason**
The outcome of the last attempt at a graceful restart. If the value is **None**, then no restart has yet been attempted. If the value is **In Progress**, then a restart attempt is currently underway. Other possible values include **Completed** (successfully completed), **Timed Out** (timed out), and **Topology Changed** (aborted due to topology change).

**Restart Helper Support**
The administrative status of the capability of an OSPFv3 router to operate in helper mode in response to a router performing a graceful restart.

**Restart Helper Strict Checking**
The administrative status of whether or not a changed Link State Advertisement (LSA) will result in termination of graceful restart by a helping router.

**Restart Helper Status**
Indicates whether the router is acting as a graceful restart helper for the neighbor.

**Time Since Exit Reason Updated**
The elapsed time since the last time the exit reason was updated.

---

**Release History**

Release 8.4.1; command introduced

---

**Related Commands**

**ipv6 ospf restart**
Configures graceful restart feature on an OSPFv3 router.

---

**MIB Objects**

- alaOspf3RestartHelperSupport
- ospfv3RestartInterval
- ospfv3RestartStatus
- ospfv3RestartAge
- ospfv3RestartExitReason
- alaOspf3RestartHelperSupport
- ospfv3RestartStrictLsaChecking
- alaOspf3RestartHelperStatus
- ospfv3RestartTime
Intermediate System-Intermediate System (IS-IS) is a shortest path first (SPF) or link-state protocol. IS-IS is an interior gateway protocol (IGP) that distributes routing information between routers in a single autonomous system (AS) for IP (IPv4 and IPv6) as well as OSI environments. This feature allows a single routing protocol to support pure IP and OSI environments, and dual environments. Integrated IS-IS is also deployed extensively in an IP-only environment.

Each participating router distributes its local state (that is, the usable interfaces of the router and reachable neighbors) throughout the AS by flooding. In a link-state protocol, each router maintains a database describing the entire AS topology. IS-IS routers have adjacencies with other routers on point-to-point links. In a multi-access network, routers report their adjacencies to a Designated Intermediate System (DIS), which generates an additional Link State PDU (LSP), commonly known as the pseudo-node LSP. The DIS is responsible for flooding the LAN with LSP and also for synchronizing the entire AS topology. This database is built from the collected link state advertisements of all routers.

IS-IS is a hierarchical protocol where the autonomous system is divided into multiple areas to reduce the size of the Routing table. Routing within an area is referred to as Level-1 routing and that between two or more areas is referred to as Level 2 routing. Each area runs a separate copy of the basic link-state routing algorithm.

The OmniSwitch version of IS-IS complies with RFC 1142.

MIB information for the IP commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-VIRTUALROUTER-MIB.mib</td>
<td>alcatelIND1VirtualRouterMIB</td>
</tr>
<tr>
<td>ALCATEL-IND1-ISIS-MIB.mib</td>
<td>timetralIsisMIBModule</td>
</tr>
<tr>
<td>ISIS-MIB.mib</td>
<td>isisMIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:
<table>
<thead>
<tr>
<th>IS-IS Commands</th>
<th>ip load isis</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip isis admin-state</td>
</tr>
<tr>
<td></td>
<td>ip isis area-id</td>
</tr>
<tr>
<td></td>
<td>ip isis level-capability</td>
</tr>
<tr>
<td></td>
<td>ip isis auth-check</td>
</tr>
<tr>
<td></td>
<td>ip isis auth-type</td>
</tr>
<tr>
<td></td>
<td>ip isis csnp-auth</td>
</tr>
<tr>
<td></td>
<td>ip isis hello-auth</td>
</tr>
<tr>
<td></td>
<td>ip isis psnp-auth</td>
</tr>
<tr>
<td></td>
<td>ip isis lsp-lifetime</td>
</tr>
<tr>
<td></td>
<td>ip isis lsp-wait</td>
</tr>
<tr>
<td></td>
<td>ip isis spf-wait</td>
</tr>
<tr>
<td></td>
<td>ip isis summary-address</td>
</tr>
<tr>
<td></td>
<td>ip isis overload</td>
</tr>
<tr>
<td></td>
<td>ip isis overload-on-boot</td>
</tr>
<tr>
<td></td>
<td>ip isis graceful-restart</td>
</tr>
<tr>
<td></td>
<td>ip isis graceful-restart helper</td>
</tr>
<tr>
<td></td>
<td>ip isis strict-adjacency-check</td>
</tr>
<tr>
<td></td>
<td>ip isis level auth-type</td>
</tr>
<tr>
<td></td>
<td>ip isis level hello-auth</td>
</tr>
<tr>
<td></td>
<td>ip isis level csnp-auth</td>
</tr>
<tr>
<td></td>
<td>ip isis level psnp-auth</td>
</tr>
<tr>
<td></td>
<td>ip isis level wide-metrics-only</td>
</tr>
</tbody>
</table>

| IPv4 and IPv6 Commands             | ip isis activate-ipv6|ipv4 |
|------------------------------------|----------------------|
|                                    | ip isis vlan         |
|                                    | ip isis vlan admin-state |
|                                    | ip isis vlan interface-type |
|                                    | ip isis vlan csnp-interval |
|                                    | ip isis vlan hello-auth-type |
|                                    | ip isis vlan level-capability |
|                                    | ip isis vlan lsp-pacing-interval |
|                                    | ip isis vlan passive |
|                                    | ip isis vlan retransmit-interval |
|                                    | ip isis vlan default-type |
|                                    | ip isis vlan level hello-auth-type |
|                                    | ip isis vlan level hello-interval |
|                                    | ip isis vlan level hello-multiplier |
|                                    | ip isis vlan level metric |
|                                    | ip isis vlan level passive |
|                                    | ip isis vlan level priority |
|                                    | ip isis summary-address6 |

<table>
<thead>
<tr>
<th>IS-IS BFD Commands</th>
<th>ip isis bfd-state</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ip isis bfd-state all-vlans</td>
</tr>
<tr>
<td></td>
<td>ip isis vlan bfd-state</td>
</tr>
<tr>
<td>Command Category</td>
<td>Commands</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Show Commands</strong></td>
<td>show ip isis adjacency</td>
</tr>
<tr>
<td></td>
<td>show ip isis database</td>
</tr>
<tr>
<td></td>
<td>show ip isis hostname</td>
</tr>
<tr>
<td></td>
<td>show ip isis routes</td>
</tr>
<tr>
<td></td>
<td>show ip isis routes6</td>
</tr>
<tr>
<td></td>
<td>show ip isis spf</td>
</tr>
<tr>
<td></td>
<td>show ip isis spf-log</td>
</tr>
<tr>
<td></td>
<td>show ip isis statistics</td>
</tr>
<tr>
<td></td>
<td>show ip isis status</td>
</tr>
<tr>
<td></td>
<td>show ip isis summary-address</td>
</tr>
<tr>
<td></td>
<td>show ip isis vlan</td>
</tr>
<tr>
<td></td>
<td>show ip isis summary-address6</td>
</tr>
<tr>
<td><strong>Clear Commands</strong></td>
<td>clear ip isis adjacency</td>
</tr>
<tr>
<td></td>
<td>clear ip isis lsp-database</td>
</tr>
<tr>
<td></td>
<td>clear ip isis spf-log</td>
</tr>
<tr>
<td></td>
<td>clear ip isis statistics</td>
</tr>
<tr>
<td><strong>M-ISIS (Multi Topology) Commands</strong></td>
<td>ip isis multi-topology</td>
</tr>
</tbody>
</table>

---

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 29-3
ip load isis

Loads the IS-IS software on the router.

ip load isis

Syntax Definitions

N/A

Defaults

By default, IS-IS is not loaded on the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- You need to load IS-IS on the switch before executing any IS-IS configuration command.
- To unload IS-IS, remove all the IS-IS configuration from “boot.cfg”.

Examples

-> ip load isis

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip protocols Displays switch routing protocol information and status.

MIB Objects

alaVrConfigTable

alaVrConfigIsisStatus
**ip isis admin-state**

Enables or disables the administrative status of IS-IS on the switch.

`ip isis admin-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables IS-IS.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables IS-IS.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900X48C6/T48C6/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900X48C4E/V48C8/C32E/T24C2/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When IS-IS status is disabled, the configuration settings and related statistics of the protocol remain unaffected.

**Examples**

```
-> ip isis admin-state enable
-> ip isis admin-state disable
```

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- `show ip isis status` Displays the IS-IS status.

**MIB Objects**

- `isisSysTable`
- `isisSysAdminState`
**ip isis area-id**

Configures the area ID for the switch.

```
ip isis area-id area address
no ip isis area-id area address
```

### Syntax Definitions

`area address`  
A 1–13 byte variable length integer, which specifies the area address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the area ID.
- The area ID is part of the Network Service Access Point (NSAP) address.
- Other parts of NSAP address (system ID and selector ID) are not configurable. System ID is derived from router ID and selector ID remains always as 00.
- You can configure a maximum of three area addresses.

### Examples

```
-> ip isis area-id 49.0001
-> no ip isis area-id 49.0001
```

### Release History

Release 7.3.3; command was introduced.
**Related Commands**

`show ip isis status`  
Displays the IS-IS status.

**MIB Objects**

`isisManAreaAddrTable`  
`isisManAreaAddrExistState`
ip isis level-capability

Configures the router level of the IS-IS protocol globally.

`ip isis level-capability {level-1 | level-2 | level-1/2}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Specifies that the router can operate at Level-1 only.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies that the router can operate at Level-2 only.</td>
</tr>
<tr>
<td>level-1/2</td>
<td>Specifies that the router can operate at both Level-1 and Level-2.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>level-1/2</td>
</tr>
<tr>
<td>level-2</td>
<td>level-1/2</td>
</tr>
<tr>
<td>level-1/2</td>
<td>level-1/2</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- Changing the level capability restarts the IS-IS protocol.
- Configuring the level capability at the IS-IS circuit level is also possible.

**Examples**

- `-> ip isis level-capability level-1`
- `-> ip isis level-capability level-2`

**Release History**

Release 7.3.3; command was introduced.
Related Commands

- **ip isis vlan level-capability** Configures the IS-IS level on the specified circuit.
- **show ip isis status** Displays the IS-IS status.

MIB Objects

- `isisSysTable`
- `isisSysType`
ip isis auth-check

Enables or disables authentication check for IS-IS PDUs.

ip isis auth-check {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables authentication check for IS-IS PDUs.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables authentication check for IS-IS PDUs.</td>
</tr>
</tbody>
</table>

Defaults

By default, authentication check is enabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If enabled, IS-IS PDUs that fail to match either of the authentication type and key requirements are rejected.
- If disabled, the authentication PDUs are generated and the IS-IS PDUs are authenticated on receipt. An error message will be generated in case of a mismatch; but PDUs will not be rejected.

Examples

- ip isis auth-check enable
- ip isis auth-check disable

Release History

Release 7.3.3; command was introduced;
**Related Commands**

- **ip isis auth-type**
  Enables authentication and configures the authentication type of IS-IS protocol globally.

- **ip isis level auth-type**
  Enables authentication and configures the authentication types for specific IS-IS levels.

- **show ip isis status**
  Displays the IS-IS status.

**MIB Objects**

- `vRtrIsisTable`
  - `vRtrIsisAuthCheck`
ip isis auth-type

Enables authentication and configures the authentication type of IS-IS protocol globally.

```
ip isis auth-type {simple {key key | encrypt-key encrypt_key} | md5 {key key | encrypt-key encrypt_key} | key-chain key_chain_id | none}
```

### Syntax Definitions

**simple**

Simple authentication will be used.

**md5**

Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.

**key**

Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.

**encrypt_key**

The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.

**key_chain_id**

The configured keychain ID.

**none**

No authentication will be used.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple</td>
<td>md5</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.

- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.

- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the `encrypt_key` parameter to configure the password by supplying the encrypted form of the password.
as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this key parameter during the CLI configuration.

- If the encrypt_key parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.

- This command configures the authentication type of IS-IS protocol globally. These settings can be overridden at each level.

- By default, the authentication is disabled and no authentication type is configured.

- If a keychain is applied globally, the authentication algorithm of its active key will be used for adjacency formation with all peers. Use ip isis auth-type none to remove the keychain from IS-IS adjacency configurations.

**Examples**

```
-> ip isis auth-type simple key rachel
-> ip isis auth-type md5 encrypt-key 7a1e441a014b4030
-> ip isis auth-type key-chain 2
```

**Release History**

Release 7.3.3; command was introduced.
Release 8.4.1; key-chain parameter added.

**Related Commands**

- **ip isis level auth-type**
  Enables authentication and configures the authentication types for specific IS-IS levels.

- **show ip isis status**
  Displays the IS-IS status.

**MIB Objects**

vRtrIsisTable

  vRtrIsisAuthType
  vRtrIsisAuthKey
  vRtrIsisAuthKeyChainId
ip isis csnp-auth

Enables or disables the authentication of Complete Sequence Number PDUs (CSNPs).

ip isis csnp-auth

no ip isis csnp-auth

Syntax Definitions

N/A

Defaults

CSNP authentication check is enabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the no form of this command to prevent the CSNP authentication.

Examples

- -> ip isis csnp-auth
- -> no ip isis csnp-auth

Release History

Release 7.3.3; command was introduced.

Related Commands

- ip isis level csnp-auth: Configures CSNP authentication for specific IS-IS levels.
- show ip isis status: Displays the IS-IS status.

MIB Objects

- vRtrIsisTable
- vRtrIsisCsnpAuthentication
**ip isis hello-auth**

Enables or disables the authentication of Hello PDUs globally.

**ip isis hello-auth**

**no ip isis hello-auth**

---

**Syntax Definitions**

N/A

**Defaults**

Authentication check of Hello PDUs is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to prevent the authentication of Hello packets.

**Examples**

- `-> ip isis hello-auth`
- `-> no ip isis hello-auth`

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

**ip isis level hello-auth** Enables or disables the authentication of Hello PDUs for specific IS-IS levels.

**show ip isis status** Displays the IS-IS status.

**MIB Objects**

vrTrTrIsisTable

vrTrTrIsisHelloAuthentication
### ip isis psnp-auth

Enables or disables the authentication of Partial Sequence Number PDUs (PSNPs).

**ip isis psnp-auth**

**no ip isis psnp-auth**

---

**Syntax Definitions**

N/A

**Defaults**

PSNP authentication check is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900</td>
</tr>
<tr>
<td>6900</td>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>9900</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **no** form of this command to prevent the authentication of PSNP packets.

**Examples**

```
-> ip isis psnp-auth
-> no ip isis psnp-auth
```

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- **ip isis level psnp-auth**
  - Configures the PSNP authentication for specific IS-IS levels.

- **show ip isis status**
  - Displays the IS-IS status.

**MIB Objects**

- **vRtrIsisTable**
  - **vRtrIsisPsnpAuthentication**
**ip isis lsp-lifetime**

Configures the time interval for which Link State PDUs generated by a router are considered valid by other routers in the same domain.

`ip isis lsp-lifetime seconds`

`no ip isis lsp-lifetime`

---

### Syntax Definitions

**seconds**

Validity interval in seconds. The valid range is 350–65535.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>1200</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

Use the `no` form of this command to restore the default value.

---

### Examples

```
-> ip isis lsp-lifetime 760
-> no ip isis lsp-lifetime
```

---

### Release History

Release 7.3.3; command was introduced.
Related Commands

**ip isis vlan lsp-pacing-interval**  Configures the interval between IS-IS LSP PDUs sent from the specified circuit.

**show ip isis status**  Displays the IS-IS status.

**show ip isis database**  Displays IS-IS LSP database information of the adjacent routers.

MIB Objects

- vRtrIsisTable
- vRtrIsisLspLifetime
ip isis lsp-wait

Configures the intervals between the first, second and subsequently generated LSPs.

`ip isis lsp-wait {max-wait | initial-wait | second-wait} seconds`

`no ip isis lsp-wait {max-wait | initial-wait | second-wait}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-wait</td>
<td>Specifies the maximum interval between two successive LSPs, in seconds. The valid range is 1–120.</td>
</tr>
<tr>
<td>initial-wait</td>
<td>Specifies the initial LSP generation delay, in seconds. The valid range is 0–100.</td>
</tr>
<tr>
<td>second-wait</td>
<td>Specifies the time interval between the first and second generated LSPs, in seconds. The valid range is 1–100.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the time interval.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds (max-wait)</td>
<td>5</td>
</tr>
<tr>
<td>seconds (initial-wait)</td>
<td>0</td>
</tr>
<tr>
<td>seconds (second-wait)</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to restore the default value.
- Successive LSPs are generated at increasing `second-wait` interval until a maximum value is reached.

**Examples**

-> `ip isis lsp-wait max-wait 25`
-> `no ip isis lsp-wait initial-wait`
**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- `ip isis vlan lsp-pacing-interval` Configures the interval between IS-IS LSP PDUs sent from the specified circuit.
- `show ip isis status` Displays the IS-IS status.

**MIB Objects**

- `vRtrIsisTable`
  - `vRtrIsisLspInitialWait`
  - `vRtrIsisLspSecondWait`
  - `vRtrIsisLspMaxWait`
**ip isis spf-wait**

Configures the intervals between the first, second, and subsequent SPF calculations.

```
ip isis spf-wait {max-wait seconds | initial-wait milliseconds| second-wait milliseconds}
no ip isis spf-wait {max-wait | initial-wait | second-wait}
```

### Syntax Definitions

- **max-wait seconds**
  Specifies the maximum interval between two successive SPF calculations, in seconds. The valid range is 1–120 seconds.

- **initial-wait milliseconds**
  Specifies the initial SPF calculation delay, in milliseconds. The valid range is 10–100000 milliseconds.

- **second-wait milliseconds**
  Specifies the interval between first and second generated SPFs, in milliseconds. The valid range is 1–100000 milliseconds.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>max-wait seconds</td>
<td>10</td>
</tr>
<tr>
<td>initial-wait milliseconds</td>
<td>1000</td>
</tr>
<tr>
<td>second-wait milliseconds</td>
<td>1000</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to restore the default value.
- Successive SPF calculations are generated at exponentially increasing **second-wait** interval until a maximum value is reached.

### Examples

```
-> ip isis spf-wait max-wait 25
-> no ip isis spf-wait initial-wait
```

### Release History

Release 7.3.3; command was introduced.
Related Commands

show ip isis status
Displays the IS-IS status.

MIB Objects

vRtrIsisTable
  vRtrIsisSpfWait
  vRtrIsisSpfInitialWait
  vRtrIsisSpfSecondWait
ip isis summary-address

Adds or deletes the summary address.

```
ip isis summary-address {ip_prefix/mask | ip_prefix [/netmask]} {level-1 | level-2 | level-1/2}
no ip isis summary-address {ip_prefix/mask | ip_prefix [/netmask]}
```

**Syntax Definitions**

- `ip_prefix/mask` Specifies the IP prefix in dotted decimal notation and the mask length.
- `ip_prefix` Specifies the IP prefix in dotted decimal notation.
- `/netmask` Specifies the subnet mask in dotted decimal notation.
- `level-1` Specifies the IS-IS level as Level-1.
- `level-2` Specifies the IS-IS level as Level-2.
- `level-1/2` Specifies the IS-IS level as Level-1/2.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>level-2</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- Use the `no` form of this command to remove an already configured summary address.
- Native IS-IS routes can only be summarized into Level-2 from the Level-1 database.
- It is not possible to summarize IS-IS internal routes at Level-1, although it is possible to summarize external (redistributed) routes at Level-1.
- IS-IS routes are not summarized by default.

**Examples**

```
-> ip isis summary-address 10.0.0.0/8 level-2
-> no ip isis summary-address 10.0.0.0/8
```
Release History
Release 7.3.3; command was introduced.

Related Commands
show ip isis summary-address  Displays the IS-IS summary address database.

MIB Objects
vRtrIIsisSummaryTable
  vRtrIIsisSummRowStatus
**ip isis overload**

Enables and configures the IS-IS router to operate in the overload state for a specified time period.

```
ip isis overload [timeout seconds]
no ip isis overload [timeout]
```

**Syntax Definitions**

```
timeout seconds  
```

Specifies the timeout interval, in seconds. The valid range is 60–1800.

**Defaults**

By default, the IS-IS overload state is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to make the router exit the overload state.
- If the time period is not specified, the router remains in the overload state for an infinite period.
- During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is used only if the destination route is directly reachable by the router i.e., it will not be used for other transit traffic.
- This command can be used when the router is overloaded or before executing a shutdown command to divert traffic around the router.

**Examples**

```
-> ip isis overload timeout 70
-> no ip isis overload timeout
```

**Release History**

Release 7.3.3; command was introduced.
Related Commands

- **ip isis overload-on-boot**
  Configures the IS-IS router to be in the overload state during bootup for a specified time period.

- **show ip isis status**
  Displays the IS-IS status.

MIB Objects

- **isisSysTable**
  - isisSysSetOverload

- **vRtrIsisTable**
  - vRtrIsisOverloadTimeout
**ip isis overload-on-boot**

Configures the IS-IS router to be in the overload state after bootup for a specified time period.

`ip isis overload-on-boot [timeout seconds]`

`no ip isis overload-on-boot [timeout seconds]`

---

**Syntax Definitions**

`timeout seconds` Specifies the timeout interval, in seconds. The valid range is 60–1800.

**Defaults**

By default, the IS-IS router will not be in the overload state.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to prevent the router from entering the overload state after bootup.
- The router in the overload state is used only if there is no alternate path to reach the destination.
- This command configures the router after bootup in the overload state until the timeout timer expires or a timeout value is specified in the `no` form of this command.
- The `no overload` command does not influence the overload-on-boot function.

**Examples**

```
-> ip isis overload-on-boot timeout 80
-> no ip isis overload-on-boot timeout
```

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

- **ip isis overload**  Sets the IS-IS router to operate in the overload state.
- **show ip isis status**  Displays the IS-IS status.

**MIB Objects**

- **vRtrIsisTable**
  - **vRtrIsisOverloadOnBoot**
  - **vRtrIsisOverloadOnBootTimeout**
**ip isis graceful-restart**

Configures graceful restart of the router. It allows routing protocols to reconverge faster, minimizing service interruption.

```
ip isis graceful-restart
no ip isis graceful-restart
```

**Syntax Definitions**

N/A

**Defaults**

Graceful restart is disabled on the router by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable graceful restart and remove the graceful restart configuration from the IS-IS router.

- When graceful restart is enabled, the router can either be a helper (which helps a neighbor router to restart) or a restarting router, or both. In the current release, only the helper mode of a router is supported.

**Examples**

```
-> ip isis graceful-restart
-> no ip isis graceful-restart
```

**Release History**

Release 7.3.3; command was introduced.
Related Commands

- **ip isis graceful-restart helper** Configures the helper mode of routers for graceful restart.
- **show ip isis status** Displays the IS-IS status.

MIB Objects

- vRtrIsisTable
  - vRtrIsisGracefulRestart
ip isis graceful-restart helper

Administratively enables and disables the IS-IS router to operate in the helper mode in response to a router performing a graceful restart.

ip isis graceful-restart helper {enable | disable}

Syntax Definitions

| enable | Enables the helper mode on the router. |
| disable | Disables the helper mode on the router. |

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When graceful restart is enabled, the helper mode is enabled by default.
- When graceful restart helper is enabled on a router, it can help other restarting routers.

Examples

```bash
-> ip isis graceful-restart helper disable
```

Release History

Release 7.3.3; command was introduced.
**Related Commands**

- `ip isis graceful-restart`  
  Configures graceful restart on the router.

- `show ip isis status`  
  Displays the IS-IS status.

**MIB Objects**

- `vRtrIsisTable`
  - `vRtrIsisGRHelperMode`
**ip isis strict-adjacency-check**

Enables or disables the adjacency check configuration on the router.

```
ip isis strict-adjacency-check {enable | disable}
```

**Syntax Definitions**

- **enable**: Enables the adjacency check configuration on the router.
- **disable**: Disables the adjacency check configuration on the router.

**Defaults**

By default, the adjacency check configuration is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the adjacency check configuration is enabled, both routers have to run the same IP version only in the IS-IS protocol to form an adjacency.
- When the adjacency check configuration is disabled, one common IP version running between two routers is enough to form an adjacency in the IS-IS protocol.

**Examples**

```
-> ip isis strict-adjacency-check enable
```

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- `show ip isis status`: Displays the IS-IS status.

**MIB Objects**

- vRtrIsisTable
  - vRtrIsisStrictAdjacencyCheck
**ip isis level auth-type**

Enables authentication and configures the authentication types for specific IS-IS levels.

```
ip isis level {1 | 2} auth-type {simple {key key | encrypt-key encrypt_key} | md5 {key key | encrypt-key encrypt_key} | key-chain key_chain_id | none}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple</td>
<td>none</td>
</tr>
<tr>
<td>md5</td>
<td>none</td>
</tr>
<tr>
<td>key-chain</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

1. Specifies the IS-IS level as Level-1.
2. Specifies the IS-IS level as Level-2.

- **simple**
  - Simple authentication will be used.
- **md5**
  - Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
  - **key**
    - Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
  - **encrypt_key**
    - The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
- **key_chain_id**
  - The configured keychain ID.
- **none**
  - No authentication will be used.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple</td>
<td>none</td>
</tr>
<tr>
<td>md5</td>
<td>none</td>
</tr>
<tr>
<td>key-chain</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.
- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
• Use the `key` parameter to configure the password for Simple or MD5 authentication. Alternatively, use the `encrypt_key` parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this `key` parameter during the CLI configuration.

• If the `encrypt_key` parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.

• This command overrides the global configuration of IS-IS authentication type.

• This command also sets the password or hash-key according to the type of authentication.

• Use `key-chain` parameter to apply a keychain to IS-IS adjacency at the capability level. Use `ip isis level auth-type none` to remove the capability level keychain authentication.

• By default, the authentication is disabled and no authentication type is configured.

**Examples**

```
-> ip isis level 2 auth-type simple key rachel
-> ip isis level 2 auth-type md5 encrypt-key 7a1e441a014b4030
-> ip isis level 2 auth-type key-chain 1
-> ip isis level 2 auth-type none
```

**Release History**

Release 7.3.3; command was introduced.
Release 8.4.1; `key-chain` parameter added.

**Related Commands**

`ip isis auth-type` Enables authentication and configures the authentication type for the IS-IS protocol globally.

`show ip isis status` Displays the IS-IS status.

**MIB Objects**

`vRtrIsisLevelTable`

  `vRtrIsisLevelAuthType`

  `vRtrIsisLevelAuthKey`

  `vRtrIsisLevel`

  `vRtrIsisLevelAuthKeyChainId`
**ip isis level hello-auth**

Enables or disables the authentication of Hello PDUs for specific IS-IS levels.

```
ip isis level {1 | 2} hello-auth
no ip isis level {1 | 2} hello-auth
```

**Syntax Definitions**

| 1 | Specifies the IS-IS level as Level-1. |
| 2 | Specifies the IS-IS level as Level-2. |

**Defaults**

Authentication check of Level Hello PDUs is enabled by default.

**Platorms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to prevent the authentication of Hello packets at the specified IS-IS level.
- This command overrides the global configuration of IS-IS Hello authentication.

**Examples**

```
-> ip isis level 1 hello-auth
-> no ip isis level 1 hello-auth
```

**Release History**

Release 7.3.3; command was introduced.
Related Commands

**ip isis hello-auth**
Enables or disables the authentication of Hello PDUs globally.

**show ip isis status**
Displays the IS-IS status.

MIB Objects

vRtrIsisLevelTable
- vRtrIsisLevelHelloAuthentication
ip isis level csnp-auth

Enables or disables the CSNP authentication for specific IS-IS levels.

ip isis level {1 | 2} csnp-auth

no ip isis level {1 | 2} csnp-auth

---

**Syntax Definitions**

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Specifies the IS-IS level as Level-1.
2. Specifies the IS-IS level as Level-2.

**Defaults**

CSNP authentication check for specific IS-IS levels is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to prevent the authentication of CSNPs at the specified IS-IS level.
- This command overrides the global configuration of IS-IS CSNP authentication.

**Examples**

- `-> ip isis level 1 csnp-auth`
- `-> no ip isis level 1 csnp-auth`

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

- `ip isis csnp-auth` Enables or disables the authentication of CSNPs.
- `show ip isis status` Displays the IS-IS status.

**MIB Objects**

- `vRtrIsisLevelTable`
  - `vRtrIsisLevelCsnpAuthentication`
**ip isis level psnp-auth**

Enables or disables PSNP authentication for specific IS-IS levels.

```
ip isis level {1 | 2} psnp-auth
no ip isis level {1 | 2} psnp-auth
```

**Syntax Definitions**

<p>| | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 1 Specifies the IS-IS level as Level-1.
- 2 Specifies the IS-IS level as Level-2.

**Defaults**

PSNP authentication check for specific IS-IS levels is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900</td>
</tr>
</tbody>
</table>

|   |   |   |   |   |   |   |   |
|---|---|---|---|---|---|---|
| No | No | No | No | Yes | Yes | Yes | Yes | Yes |

**Usage Guidelines**

- Use the **no** form of this command to prevent the authentication of PSNPs at the specified IS-IS level.
- This command overrides the global configuration of IS-IS PSNP authentication.

**Examples**

```
-> ip isis level 1 psnp-auth
-> no ip isis level 1 psnp-auth
```

**Release History**

Release 7.3.3; command was introduced.
Related Commands

- **ip isis psnp-auth**: Enables or disables the authentication of PSNPs.
- **show ip isis status**: Displays the IS-IS status.

MIB Objects

- **vRtrIsisLevelTable**
  - **vRtrIsisLevelPsnpAuthentication**
**ip isis level wide-metrics-only**

Enables the wide metrics in LSPs for specific IS-IS levels.

```
ip isis level {1 | 2} wide-metrics-only
no ip isis level {1 | 2} wide-metrics-only
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th></th>
<th>Specifies the IS-IS level as Level-1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

By default, wide metrics is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- Use the `no` form of this command to restore the narrow metric (1–63).
- Wide metrics are used for improved granularity of metrics.
- Numeric values above 63 indicate wide metrics.

**Examples**

```
-> ip isis level 1 wide-metrics-only
-> no ip isis level 1 wide-metrics-only
```

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

- **show ip isis status**
  Displays the IS-IS status.

**MIB Objects**

- **vrtrisisLevelTable**
  - **VrtrIisisLevelWideMetricsOnly**
ip isis activate-ipv6|ipv4

Configures the IPv6 or IPv4 routing in IS-IS.

ip isis {activate-ipv6 | activate-ipv4}

no ip isis {activate-ipv6 | activate-ipv4}

Syntax Definitions

activate-ipv6       Enables IPv6 routing in IS-IS.
activate-ipv4       Enables IPv4 routing in IS-IS.

Defaults

By default, both IPv4 and IPv6 routing is enabled in IS-IS.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The no form of this command disables the IPv4/IPv6 routing in IS-IS.

Examples

-> ip isis activate-ipv6
-> ip isis activate-ipv4
-> no ip isis activate-ipv4

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis status       Displays the IS-IS status.

MIB Objects

vRtrIsisActivateIPV4
vRtrIsisActivateIPV6
ip isis vlan

Configures IPv4 or IPv6 IS-IS circuit on a particular VLAN. This command enables IS-IS routing on a particular VLAN. This is used to add both the IPv4 and IPv6 interfaces on a particular VLAN to the IS-IS circuit.

ip isis vlan vlan_id [address-family {v4 | v6 | v4v6}]

Syntax Definitions

- **vlan_id**: The VLAN ID of a given VLAN on which IS-IS is to be enabled.
- **v4 | v6 | v4v6**: The address family extension. The type of interface (IPv4 or IPv6) is controlled by the address-family extension.

Defaults

By default, both address families (IPv4 and IPv6) are disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The no form of this command disables IPv4/IPv6 IS-IS circuit on a particular VLAN.

Examples

- -> ip isis vlan 10
- -> ip isis vlan 10 address-family v6
- -> no ip isis vlan 10 address-family v6

Release History

Release 7.3.3; command was introduced.
Related Commands

show ip isis vlan  Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

vRtrIsisIfTable
  vRtrIsisIfRowStatus
**ip isis vlan admin-state**

Enables or disables IS-IS on a circuit.

`ip isis vlan vlan_id admin-state {enable | disable}`

**Syntax Definitions**

- `vlan_id`: The VLAN ID of a given VLAN on which IS-IS routing is to be enabled.
- `enable`: Administratively enables IS-IS on the VLAN.
- `disable`: Administratively disables IS-IS on the VLAN.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the status is manually disabled, the configuration settings and related statistics of the protocol remain unaffected.

**Examples**

- `-> ip isis vlan 10 admin-state enable`
- `-> ip isis vlan 10 admin-state disable`

**Release History**

Release 7.3.3; command was introduced.
Related Commands

show ip isis vlan

Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

isisCircTable
  isisCircAdminState
**ip isis vlan interface-type**

Configures the IS-IS interface (circuit) type as broadcast or point-to-point.

`ip isis vlan vlan_id interface-type {broadcast | point-to-point}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>The VLAN ID of a given VLAN.</td>
</tr>
<tr>
<td><code>broadcast</code></td>
<td>Sets the interface (circuit) type as a broadcast IS-IS interface.</td>
</tr>
<tr>
<td><code>point-to-point</code></td>
<td>Sets the interface (circuit) type as a point-to-point IS-IS interface.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>broadcast</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `-> ip isis vlan 10 interface-type broadcast`
- `-> ip isis vlan 10 interface-type point-to-point`

**Release History**

Release 7.3.3; command was introduced.
Related Commands

- **ip isis vlan default-type**
  Sets the interface type to default, that is, broadcast.

- **show ip isis vlan**
  Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

- **isisCircTable**
- **isisCircType**
ip isis vlan csnp-interval

Configures the time interval in seconds to send Complete Sequence Number PDUs (CSNP) PDUs from the specified VLAN circuit.

**ip isis vlan vlan_id csnp-interval seconds**

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id</td>
<td>The VLAN ID of a given VLAN.</td>
</tr>
<tr>
<td>seconds</td>
<td>The time interval in seconds between successive CSNP PDUs sent on an interface after which IS-IS must generate a CSNP PDU on the specified circuit. The valid range is 1–65535.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Broadcast interface: 10 seconds</td>
</tr>
<tr>
<td></td>
<td>Point-to-Point interface: 5 seconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The no form of this command reverts the time interval to the default value.

**Examples**

- `-> ip isis vlan 10 csnp-interval 10`
- `-> no ip isis vlan 10 csnp-interval`

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

*show ip isis status*  
Displays the IS-IS status.

**MIB Objects**

vRtrIsisIfCsnpInterval
### ip isis vlan hello-auth-type

Configures the authentication settings for the hello protocol at a circuit level.

```
ip isis vlan vlan_id hello-auth-type {simple {key key | encrypt-key encrypt_key} | md5 {key key | encrypt-key encrypt_key} | key-chain key_chain_id | none}
```

#### Syntax Definitions

- **vlan_id**: The VLAN ID of a given VLAN.
- **simple**: Simple authentication will be used.
- **md5**: Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
- **key**: Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
- **encrypt_key**: The key in hexadecimal format to provide security considerations on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
- **key_chain_id**: The configured keychain ID.
- **none**: No authentication will be used.

#### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple</td>
<td>md5</td>
</tr>
</tbody>
</table>

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.

- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.
• Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the encrypt_key parameter to configure the password by supplying the encrypted form of the password as the encrypt_key. The Configuration snapshot always displays the password in the encrypted form. You must use only this key parameter during the CLI configuration.

• If the encrypt_key parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt_key.

• Use key-chain parameter to apply a keychain at a circuit level. Use `ip isis vlan hello-auth-type none` to remove the circuit level keychain authentication.

• By default, the authentication is disabled and no authentication type is configured.

Examples

-> ip isis vlan 10 hello-auth-type md5 key asddfgfhno
-> ip isis vlan 10 hello-auth-type simple key sdsdff
-> ip isis vlan 100 hello-auth-type key-chain 1
-> ip isis vlan 100 hello-auth-type none

Release History

Release 7.3.3; command was introduced.
Release 8.4.1; `key-chain` parameter added.

Related Commands

`ip isis vlan level hello-auth-type` Configures the authentication of Hello PDUs for the specified IS-IS level of an IS-IS Circuit.

`show ip isis vlan` Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

vRtrIsisIfHelloAuthKey
vRtrIsisIfHelloAuthType
vRtrIsisIfHelloAuthKeyChainId
ip isis vlan level-capability

Configures the IS-IS level on the specified circuit.

```
ip isis vlan vlan_id level-capability [level-1 | level-2 | level-1/2]
```

**Syntax Definitions**

- **vlan_id**
  - The VLAN ID of a given VLAN.

- **level-1**
  - Specifies that the interface can operate at Level-1 only.

- **level-2**
  - Specifies that the interface can operate at Level-2 only.

- **level-1/2**
  - Specifies that the interface can operate at both Level-1 and Level-2.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1/2</td>
<td>level-1/2</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Changing the level capability restarts the IS-IS protocol on the interface.

- If the level capability is configured globally and on a specific interface, the combination of the two settings will decide the potential adjacency.

**Examples**

```
-> ip isis vlan 10 level-capability level-1
-> ip isis vlan 10 level-capability level-1/2
```

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

- **ip isis level-capability**
  Configures the router level of the IS-IS protocol globally.

- **show ip isis vlan**
  Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

**MIB Objects**

- **isisCircTable**
  - **isisCircLevel**
ip isis vlan lsp-pacing-interval

Configures the interval between IS-IS LSP PDUs sent from the specified circuit.

ip isis vlan vlan_id lsp-pacing-interval milliseconds

no ip isis vlan vlan_id lsp-pacing-interval

Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliseconds</td>
<td>100</td>
</tr>
</tbody>
</table>

Defaults

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to restore the default settings.
- No LSPs are sent from the specified interface if the time interval is set to 0.

Examples

- -> ip isis vlan 10 lsp-pacing-interval 1000
- -> no ip isis vlan 10 lsp-pacing-interval

Release History

Release 7.3.3; command was introduced.
**Related Commands**

- **ip isis lsp-lifetime**
  Configures the time interval for which LSPs generated by a router is considered valid by other routers in the same domain.

- **ip isis lsp-wait**
  Configures the time interval between successively generated LSPs.

- **show ip isis vlan**
  Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

**MIB Objects**

- `vRtrIsisIfTable`
  - `vRtrIsisIfLspPacingInterval`
ip isis vlan passive

Configures the IS-IS circuit as passive.

ip isis vlan vlan_id passive

no ip isis vlan vlan_id passive

Syntax Definitions

vlan_id

The VLAN ID of a given VLAN.

Defaults

By default, the interface is not passive.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the passive attribute.
- This command adds the passive attribute that causes the IS-IS circuit to be advertised as an IS-IS circuit without running the IS-IS protocol. Normally, only interface addresses that are configured for IS-IS are advertised as IS-IS interface at the level that they are configured. When the passive mode is enabled, the interface or the interface at the level ignores ingress IS-IS PDUs (Protocol Data Unit) and will not transmit IS-IS protocol PDUs.

Examples

- ip isis vlan 10 passive
- no ip isis vlan 10 passive

Release History

Release 7.3.3; command was introduced.
Related Commands

- `ip isis vlan level passive` Configures the IS-IS circuit as passive at the specified IS-IS level.
- `show ip isis vlan` Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

- `isisCircTable`
  - `isisCircPassiveCircuit`
**ip isis vlan retransmit-interval**

Configures the minimum time interval between LSP (Link State Packet) retransmissions on a point-to-point interface.

`ip isis vlan vlan_id retransmit-interval seconds`

`no ip isis vlan vlan_id retransmit-interval`

**Syntax Definitions**

- `vlan_id` The VLAN ID of a given VLAN.
- `seconds` The minimum time interval (1–65535) in seconds between LSP transmissions on a point-to-point interface.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>5</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to restore the default settings.
- The retransmit interval should be greater than the expected round-trip delay between two devices to avoid any needless retransmission of PDUs.

**Examples**

- `-> ip isis vlan 10 retransmit-interval 130`
- `-> no ip isis vlan 10 retransmit-interval`

**Release History**

Release 7.3.3; command was introduced.
Related Commands

show ip isis vlan         Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

vRtrIsisIfTbale
- vRtrIsisIfRetransmitInterval
**ip isis vlan default-type**

Sets the interface type to default, that is, broadcast.

```
ip isis vlan vlan_id default-type
```

### Syntax Definitions

- `vlan_id` The VLAN ID of a given VLAN.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> ip isis vlan 10 default-type
```

### Release History

Release 7.3.3; command was introduced.

### Related Commands

- **ip isis vlan interface-type** Configures the IS-IS interface (circuit) type as broadcast or point-to-point.

### MIB Objects

- `vRtrIsisIfTable`
  - `vRtrIsisIfTypeDefault`
ip isis vlan level hello-auth-type

Configures the authentication of Hello PDUs for the specified IS-IS level of an IS-IS Circuit.

```
ip isis vlan vlan_id level {1 | 2} hello-auth-type {simple {key key | encrypt-key encrypt_key} | md5 {key key | encrypt-key encrypt_key} | key-chain key_chain_id | none}
```

**Syntax Definitions**

- `vlan_id`: The VLAN ID of a given VLAN.
- `1`: Specifies the IS-IS level as Level-1.
- `2`: Specifies the IS-IS level as Level-2.
- `simple`: Simple authentication will be used.
- `md5`: Specifies that MD5 authentication algorithm will be used. Hash-key will be used in MD5 authentication.
- `key`: Key will be plain text ASCII up to 118 characters. Use quotes around string if the key contains multiple words with spaces between them.
- `encrypt_key`: The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form.
- `key_chain_id`: The configured keychain ID.
- `none`: No authentication will be used.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple</td>
<td>none</td>
</tr>
<tr>
<td>md5</td>
<td>none</td>
</tr>
<tr>
<td>key-chain</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Simple authentication uses only a text string as the password in the packet. This helps to protect the routers from a configuration mishap. MD5 authentication is used to protect the system from malicious actions.

- MD5 authentication is used to encrypt the information that is sent over the network. MD5 authentication uses shared secret key. The Key is used to sign the packets with an MD5 checksum to
sign the packet, so that the packets cannot be tampered. As the key is not included in the packet, snooping the key is not possible.

- Use the Key parameter to configure the password for Simple or MD5 authentication. Alternatively, use the encrypt_key parameter to configure the password by supplying the encrypted form of the password as the encrypt-key. The Configuration snapshot always displays the password in the encrypted form. You should use only this key parameter during the CLI configuration.

- If the encrypt_key parameter is used to configure the password through the CLI, then its value should be the same as the one that appears in the configuration snapshot. Only valid system generated values are accepted as encrypt-key.

- This command also configures the authentication type and the corresponding key. These settings override the configuration done at an interface level.

- Use key-chain parameter to apply a keychain at the capability level per circuit. Use ip isis vlan level hello-auth-type none to remove the capability level keychain authentication per circuit.

- By default, the authentication is disabled and no authentication type is configured.

**Examples**

-> ip isis vlan 10 level 1 hello-auth-type md5 key xyz123
-> ip isis vlan 10 level 2 hello-auth-type none
-> ip isis vlan 100 level 2 hello-auth-type key-chain 1
-> ip isis vlan 100 level 2 hello-auth-type none

**Release History**

Release 7.3.3; command was introduced.
Release 8.4.1; key-chain parameter added.

**Related Commands**

- **ip isis vlan hello-auth-type** Configures the authentication settings for the hello protocol at a circuit level.

- **show ip isis vlan** Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

**MIB Objects**

vRtrIsisIfLevelTable
  vRtrIsisIfLevelHelloAuthType
  vRtrIsisIfLevelHelloAuthKey
  vRtrIsisIfLevel
  vRtrIsisIfLevelHelloAuthKeyChainId
ip isis vlan level hello-interval

Configures the time interval between the successive Hello PDUs for the specified IS-IS level on a circuit.

**ip isis vlan vlan_id level {1 | 2} hello-interval seconds**

**no ip isis vlan vlan_id level {1 | 2} hello-interval**

### Syntax Definitions

- **vlan_id**
  - The VLAN ID of a given VLAN.
- **1**
  - Specifies the IS-IS level as Level-1.
- **2**
  - Specifies the IS-IS level as Level-2.
- **seconds**
  - The hello interval, in seconds. The valid range is 1–20000.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds (designated routers)</td>
<td>3</td>
</tr>
<tr>
<td>seconds (non-designated routers)</td>
<td>9</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **no** form of this command to restore the default settings.

### Examples

- `-> ip isis vlan 10 level 1 hello-interval 50`
- `-> no ip isis vlan 10 level 2 hello-interval`

### Release History

Release 7.3.3; command was introduced.
Related Commands

**show ip isis vlan**  Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

vRtrIsisIfLevelTable  vRtrIsisIfLevelHelloTimer
**ip isis vlan level hello-multiplier**

Configures the number of missing Hello PDUs from a neighbor, after which the adjacency is declared as down.

```
ip isis vlan vlan_id level {1 | 2} hello-multiplier number
no ip isis vlan vlan_id level {1 | 2} hello-multiplier
```

### Syntax Definitions

- **vlan_id**: The VLAN ID of a given VLAN.
- **1**: Specifies the IS-IS level as Level-1.
- **2**: Specifies the IS-IS level as Level-2.
- **number**: The multiplier (2–100) of the hello interval.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>3</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `no` form of this command to restore the default settings.

### Examples

```
-> ip isis vlan 10 level 1 hello-multiplier 10
-> no ip isis vlan 10 level 2 hello-multiplier
```

### Release History

Release 7.3.3; command was introduced.
Related Commands

show ip isis vlan

Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

isisCircLevelTable
isisCircLevelHelloMultiplier
**ip isis vlan level metric**

Configures the metric value of the specified IS-IS level of the circuit.

```
ip isis vlan vlan_id level {1 | 2} metric number
no ip isis vlan vlan_id level {1 | 2} metric
```

**Syntax Definitions**

- `vlan_id`: The VLAN ID of a given VLAN.
- `1`: Specifies the IS-IS level as Level-1.
- `2`: Specifies the IS-IS level as Level-2.
- `number`: The metric value (1–16777215) assigned for the specified level of the circuit.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>10</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to restore the default value.
- To calculate the lowest cost to reach a destination, each configured level on each circuit must have a cost. The costs for each level on a circuit may be different. If the metric is not configured, the default of 10 is used.

**Examples**

```
-> ip isis vlan 10 level 1 metric 25
-> no ip isis vlan 10 level 2 metric
```

**Release History**

Release 7.3.3; command was introduced.
Related Commands

**show ip isis vlan**

Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

- `vRtrIsisIfLevelTable`
- `vRtrIsisIfLevelAdminMetric`
**ip isis vlan level passive**

Configures the IS-IS circuit as passive at the specified IS-IS level.

```
ip isis vlan vlan_id level {1 | 2} passive
no ip isis vlan vlan_id level {1 | 2} passive
```

**Syntax Definitions**

- `vlan_id` The VLAN ID of a given VLAN.
- `1` Specifies the IS-IS level as Level-1.
- `2` Specifies the IS-IS level as Level-2.

**Defaults**

By default, the interface level passive configuration is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the passive attribute.
  - This command adds the passive attribute that causes the IS-IS circuit at the given level to be advertised as an IS-IS circuit without running the IS-IS protocol. Normally, only interface addresses that are configured for IS-IS are advertised as IS-IS interface at the level that they are configured. When the passive mode is enabled, the interface or the interface at the level ignores ingress IS-IS protocol PDUs and will not transmit IS-IS protocol PDUs.

**Examples**

```
-> ip isis vlan 10 level 1 passive
-> no ip isis vlan 10 level 1 passive
```

**Release History**

Release 7.3.3; command was introduced.
Related Commands

- **ip isis vlan passive**: Configures the IS-IS circuit as passive.
- **show ip isis vlan**: Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

MIB Objects

- **vRtrIsisIfLevelTable**
- **vRtrIsisIfLevelPassive**
ip isis vlan level priority

Configures the priority of the IS-IS circuit for the designated router election on a multi-access network.

```
ip isis vlan vlan_id level [1 | 2] priority number
no ip isis vlan vlan_id level [1 | 2] priority
```

**Syntax Definitions**

- `vlan_id`: The VLAN ID of a given VLAN.
- `1`: Specifies the IS-IS level as Level-1.
- `2`: Specifies the IS-IS level as Level-2.
- `number`: The priority value of the IS-IS circuit at this level. The valid range is 0–127.

**Defaults**

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>64</td>
</tr>
</tbody>
</table>
```

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- Use the `no` form of this command to restore the default value.
- This priority is included in hello PDUs transmitted by the circuit on a multi-access network.
- The router with the highest priority is the preferred designated router.
- The designated router sends LSPs to this network and also to the routers that are attached to it.

**Examples**

```
-> ip isis vlan 10 level 1 priority 4
-> ip isis vlan 10 level 2 priority 4
-> no ip isis vlan 10 level 1 priority
```

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

`show ip isis vlan` Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

**MIB Objects**

- `vRtrIsisIfLevelTable`
- `vRtrIsisIfLevelISPriority`
ip isis summary-address6

Configures the IPv6 summary address.

ip isis summary-address6 {ipv6_prefix/prefix_length | ipv6_address} {level-1 | level-2 | level-1/2}

no ip isis summary-address6 {ipv6_prefix/prefix_length | ipv6_address} {level-1 | level-2 | level-1/2}

**Syntax Definitions**

- `ipv6_prefix/prefix_length`: IPv6 prefix and prefix length.
- `ipv6_address`: IPv6 address.
- `level-1`: Specifies that the routes can be summarized at Level-1 only.
- `level-2`: Specifies that the routes can be summarized at Level-2 only.
- `level-1/2`: Specifies that the routes can be summarized at both Level-1 and Level-2.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to remove an already configured summary address.

**Examples**

- `-> ip isis summary-address6 4001::/16 level-1`
- `-> no ip isis summary-address6 4001::/16`

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

*show ip isis summary-address6* Displays the IS-IS IPv6 summary address database.

**MIB Objects**

- `vRtrIsisInetSummLevel`
- `vRtrIsisInetSummRowStatus`
ip isis bfd-state

Enables or disables the registration of IS-IS with the BFD protocol.

ip isis bfd-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for IS-IS.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for IS-IS.</td>
</tr>
</tbody>
</table>

Defaults

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- BFD must be globally enabled for the switch and IS-IS must be registered with BFD at the protocol level before IS-IS can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and IS-IS acts based upon the BFD message.
- Whenever a neighbor goes down, IS-IS will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

-> ip bfd admin-state enable

Enables and disables the registration of IS-IS with the BFD protocol:

-> ip isis bfd-state enable
-> ip isis bfd-state disable

Release History

Release 8.4.1.R03; command was introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip bfd admin-state</td>
<td>Enables or disables the global BFD protocol status for the switch.</td>
</tr>
<tr>
<td>ip isis bfd-state all-vlans</td>
<td>Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.</td>
</tr>
<tr>
<td>ip isis vlan bfd-state</td>
<td>Enables or disables BFD monitoring on a specific PIM interface.</td>
</tr>
<tr>
<td>show ip isis status</td>
<td>Displays the IS-IS status.</td>
</tr>
</tbody>
</table>

### MIB Objects

- vRtrIsisIfTable
  - vRtrIsisBfdStatus
**ip isis bfd-state all-vlans**

Enables or disables BFD monitoring for all IS-IS VLANs in the switch configuration.

```
ip isis bfd-state all-vlans {enable | disable}
```

### Syntax Definitions

- **enable**: Enables BFD for all the IS-IS VLANs.
- **disable**: Disables BFD for all the IS-IS VLANs.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The BFD status for IS-IS must be enabled before IS-IS can interact with BFD.

### Examples

- `-> ip isis bfd-state all-vlans enable`
- `-> ip isis bfd-state all-vlans disable`

### Release History

Release 8.4.1.R03; command was introduced.

### Related Commands

- **ip isis bfd-state**: Enables or disables the registration of IS-IS with the BFD protocol.
- **ip isis vlan bfd-state**: Enables or disables BFD monitoring on a specific IS-IS VLAN.
- **show ip isis vlan**: Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

### MIB Objects

- **vRtrIsisTable**
- **vRtrIsisBfdAllVlanStatus**
ip isis vlan bfd-state

Enables or disables BFD monitoring for a specific IS-IS VLAN.

```
ip isis vlan vlan_id bfd-state {enable | disable}
```

**Syntax Definitions**

- `vlan_id` The VLAN ID of a given VLAN.
- `enable` Enables BFD for the specified IS-IS VLAN.
- `disable` Disables BFD for the specified IS-IS VLAN.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Registering IS-IS with BFD is required at the protocol level before IS-IS can interact with BFD.
- When BFD is enabled on the specified IS-IS VLAN, BFD is applied to all IPv4 and IPv6 interfaces configured for the VLAN.
- A single IS-IS adjacency covers both IPv4 and IPv6 interfaces, but the interfaces are treated independently within the adjacency. If an IS-IS adjacency has both interface types, there will be two BFD sessions (one for each interface). When one interface goes down, only the routes learned through that interface are removed.

**Examples**

```
-> ip isis vlan 10 bfd-state enable
-> ip isis vlan 10 bfd-state disable
```

**Release History**

Release 8.4.3.R03; command was introduced.
**Related Commands**

- `ip isis bfd-state` Enables or disables the registration of IS-IS with the BFD protocol.
- `ip isis bfd-state all-vlans` Enables or disables BFD monitoring for all IS-IS interfaces in the switch configuration.
- `show ip isis vlan` Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

**MIB Objects**

- `vRtrIsisIfTable`
  - `vRtrIsisIfBfdStatus`
show ip isis adjacency

Displays information about IS-IS adjacent routers.

```
show ip isis adjacency [{system-id nbr_sys_id | vlan vlan_id}] [detail]
```

### Syntax Definitions

- `nbr_sys_id`: The system ID of the neighbor router.
- `vlan_id`: The VLAN ID of a given VLAN.

### Defaults

By default adjacency information for all the neighbor routers are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `nbr_sys_id` or `vlan_id` parameter with this command to view the adjacency information for a specific neighbor.

### Examples

```
-> show ip isis adjacency
==============================================================
ISIS Adjacency
==============================================================
System ID | Type | State | Hold | VlanID | MT IDs | Hostname
----------|------|-------|------|--------|--------|----------
0000.0000.0001 | L1 | UP    | 25   | 20     | 0, 2   | Router-A
0000.0000.0002 | L2 | UP    | 21   | 30     | None   | Router-B

Adjacency : 2
==============================================================
```

### output definitions

- **System ID**: The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.
- **Type**: The level (L1, L2, or L1/L2) of the adjacent router.
- **State**: The state of the adjacent router (Up or Down).
output definitions

| SystemID | The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID. |
| VLAN | MT IDs
| The VLAN ID in which the adjacency is present. | MT IDs sent by MT enabled ISIS neighbor. '0' signifies the IPv4 support, '2' signifies IPv6 support, 'none' signifies MT disabled neighbor. |
| NLPIDs | The IP address families supported by IS-IS neighbor: IPv4 or IPv6 |

SystemID : 0000.0000.0001  SNPA : 00:d0:95:f3:0f:08
VLAN : 20  Up Time : WED JUN 05 05:18:51 2013
State : UP  Priority : 64
Nbr Sys Type : L2  L.CircType : L1L2
Hold Time : 6  Max Hold : 9
Adj Level : L2  Host-name : Router-A
MT IDs : 0, 2  NLPIDs : IPv4, IPv6
IPv4 Neighbor : 2.2.2.3
IPv6 Neighbor : FE80::C809:FFF:FEDC:0
Restart Support : Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled

SystemID : 0000.0000.0002  SNPA : 00:d0:95:f3:0f:08
VLAN : 10  Up Time : WED JUN 05 05:18:51 2013
State : UP  Priority : 64
Nbr Sys Type : L1  L.CircType : L1L2
Hold Time : 6  Max Hold : 9
Adj Level : L2  Host-name : Router-B
MT IDs : None  NLPIDs : IPv4
IPv4 Neighbor : 2.2.2.3
IPv6 Neighbor : FE80::C809:AFF:FEEC:0
Restart Support : Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled

Adacency : 2

output definitions

| SystemID | The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID. |
| VLAN | MT IDs
| The VLAN ID in which the adjacency is present. | MT IDs sent by MT enabled ISIS neighbor. '0' signifies the IPv4 support, '2' signifies IPv6 support, 'none' signifies MT disabled neighbor. |
| NLPIDs | The IP address families supported by IS-IS neighbor: IPv4 or IPv6 |

SystemID : 0000.0000.0001  SNPA : 00:d0:95:f3:0f:08
VLAN : 20  Up Time : WED JUN 05 05:18:51 2013
State : UP  Priority : 64
Nbr Sys Type : L2  L.CircType : L1L2
Hold Time : 6  Max Hold : 9
Adj Level : L2  Host-name : Router-A
MT IDs : 0, 2  NLPIDs : IPv4, IPv6
IPv4 Neighbor : 2.2.2.3
IPv6 Neighbor : FE80::C809:FFF:FEDC:0
Restart Support : Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled

SystemID : 0000.0000.0002  SNPA : 00:d0:95:f3:0f:08
VLAN : 10  Up Time : WED JUN 05 05:18:51 2013
State : UP  Priority : 64
Nbr Sys Type : L1  L.CircType : L1L2
Hold Time : 6  Max Hold : 9
Adj Level : L2  Host-name : Router-B
MT IDs : None  NLPIDs : IPv4
IPv4 Neighbor : 2.2.2.3
IPv6 Neighbor : FE80::C809:AFF:FEEC:0
Restart Support : Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled

Adacency : 2

output definitions

| SystemID | The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID. |
| VLAN | MT IDs
| The VLAN ID in which the adjacency is present. | MT IDs sent by MT enabled ISIS neighbor. '0' signifies the IPv4 support, '2' signifies IPv6 support, 'none' signifies MT disabled neighbor. |
| NLPIDs | The IP address families supported by IS-IS neighbor: IPv4 or IPv6 |

SystemID : 0000.0000.0001  SNPA : 00:d0:95:f3:0f:08
VLAN : 20  Up Time : WED JUN 05 05:18:51 2013
State : UP  Priority : 64
Nbr Sys Type : L2  L.CircType : L1L2
Hold Time : 6  Max Hold : 9
Adj Level : L2  Host-name : Router-A
MT IDs : 0, 2  NLPIDs : IPv4, IPv6
IPv4 Neighbor : 2.2.2.3
IPv6 Neighbor : FE80::C809:FFF:FEDC:0
Restart Support : Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled

SystemID : 0000.0000.0002  SNPA : 00:d0:95:f3:0f:08
VLAN : 10  Up Time : WED JUN 05 05:18:51 2013
State : UP  Priority : 64
Nbr Sys Type : L1  L.CircType : L1L2
Hold Time : 6  Max Hold : 9
Adj Level : L2  Host-name : Router-B
MT IDs : None  NLPIDs : IPv4
IPv4 Neighbor : 2.2.2.3
IPv6 Neighbor : FE80::C809:AFF:FEEC:0
Restart Support : Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled

Adacency : 2
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The state of the adjacent router (Up or Down).</td>
</tr>
<tr>
<td>Adj Level</td>
<td>The adjacency level (L1 or L2) of the router.</td>
</tr>
<tr>
<td>Nbr Sys Type</td>
<td>The type of the neighboring router (L1, L2 or L1L2)</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The Hold time of the adjacent router.</td>
</tr>
<tr>
<td>IPv4 Neighbor</td>
<td>The 32-bit IP address of the neighbor.</td>
</tr>
<tr>
<td>IPv6 Neighbor</td>
<td>The 32-bit IPv6 address of the neighbor</td>
</tr>
<tr>
<td>Restart Support</td>
<td>Indicates if graceful restart is enabled or disabled.</td>
</tr>
<tr>
<td>Restart Status</td>
<td>Indicates whether the router is currently helping an adjacent router to restart.</td>
</tr>
<tr>
<td>Restart Suppressed</td>
<td>Indicates whether the advertisement of LSPs are suppressed (enabled) or not (disabled) as per the request of adjacent router.</td>
</tr>
<tr>
<td>SNPA</td>
<td>The SNPA address of the adjacent router.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Indicates the time period in seconds, during which the router was in the adjacency.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of the adjacent router.</td>
</tr>
<tr>
<td>Host-name</td>
<td>The host name of the adjacent router.</td>
</tr>
<tr>
<td>L. CircType</td>
<td>Indicates the level circuit type (L1, L2 or L1L2) of the adjacent router.</td>
</tr>
<tr>
<td>Max Hold</td>
<td>Indicates the maximum Hold time of the adjacent router.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

`clear ip isis adjacency` Clears and resets the IS-IS adjacency database.

**MIB Objects**

- isisISAdjTable
  - isisISAdjIndex
  - isisISAdjState
  - isisISAdjNeighSNPAAddress
  - isisISAdjNeighSysType
  - isisISAdjNeighSysID
  - isisISAdjUsage
  - isisISAdjNeighPriority
  - isisISAdjUpTime
  - isisISAdjHoldTimer
- vRtrIisisISAdjTable
  - vRtrIisisISAdjCircLevel
  - vRtrIisisISAdjRestartSupport
  - vRtrIisisISAdjRestartSuppressed
  - vRtrIisisISAdjExpireIn
  - vRtrIisisISAdjNeighborIP
  - vRtrIisisISAdjRestartStatus
vRtrIsisISAdjMTIdMask
**show ip isis database**

Displays IS-IS LSP database information of the adjacent routers.

`show ip isis database [\{system_id system_id | lsp_id lsp_id\} \[detail\] \[level \{1 | 2\}\]`

### Syntax Definitions

- `system_id` The system ID of the router.
- `lsp_id` The LSP ID.
- `detail` Indicates that the output is displayed in a detailed manner.
- `level` Indicates the IS-IS level, either 1 or 2.

### Defaults

By default, the entire LSP database is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use `system_id` or `lsp_id` parameter with this command to view specific LSP database information.
- Use the `level` parameter with this command to view the LSP database information of a particular level.

### Examples

```
-> show ip isis database
Legends : P    = The Partition repair bit is set
          OV   = The overload bit is set
          ATT  = The Attach bit is set
          L1   = Specifies a Level 1 IS type
          L2   = Specifies a Level 2 IS type

===============================================================
ISIS Database
===============================================================
LSP ID                        Sequence Checksum Lifetime Attributes
===============================================================
Displaying level-1 database
........................................................................
1720.2116.0051.00-00          0x44   0xb664   919   L1L2
level-1 LSP count : 1
```
Displaying level-2 database
------------------------------------------------------------------
1720.2116.0051.00-00  0x45  0xb465  1083  L1L2
level-2 LSP count : 1
==================================================================

output definitions

<table>
<thead>
<tr>
<th>LSP ID</th>
<th>The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence</td>
<td>The sequence number of the LSP. The sequence number is a value used to identify old and duplicate LSPs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>The checksum value of the LSP.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the Link State Database of all the routers.</td>
</tr>
<tr>
<td>Attributes</td>
<td>The level capability of the router.</td>
</tr>
<tr>
<td>LSP Count</td>
<td>The number of LSPs in the Link State Database.</td>
</tr>
</tbody>
</table>

--> show ip isis database detail
   Legends : P    =  The Partition repair bit is set
              OV   =  The overload bit is set
              ATT  =  The Attach bit is set
              L1    =  Specifies a Level 1 IS type
              L2    =  Specifies a Level 2 IS type

ISIS Database
==================================================================
Displaying level-1 database
------------------------------------------------------------------
LSP ID      :  1720.2116.0051.00-00   Level      :  L1
Sequence    :  0x44                  Checksum  :  0xb664   Lifetime  :  818
Version     :  1                      Pkt Type   :  18     Pkt Ver   :  1
Attributes  :  L1L2                  Max Area   :  3
SysID Len   :  6                      Used Len   :  635    Alloc Len :  1489

TLVs :
Area Addresses :
   Area Address  :  (3)  49.0000
Supp protocols :
   Protocols     :  Ipv4, Ipv6
IS-Hostname :
   Hostname      :  HostA
IS Neighbors :
   Virtual Flag  :  0
   Neighbor      :  1720.2116.0052.00  Metric :  10 (I)
IPV4 I/F Address :
   IP Address     :  172.21.160.51
   IP Address     :  172.21.160.52
IPV6 I/F Address :
   IPv6 Address   :  2001:1::1
   IPv6 Address   :  3001:1::1
IPV4 Internal Reach :
   IP Prefix      :  16.16.16.0/24 (Dir.: UP )  Metric :  10 (I)
   IP Prefix      :  17.17.17.0/24 (Dir.: UP )  Metric :  10 (I)
IPv4 External Reach:
  IP Prefix       : 24.24.24.0/24 (Dir.: UP ) Metric  : 10 (E)
  IP Prefix       : 25.25.25.0/24 (Dir.: UP ) Metric  : 10 (E)
IPv6 Reach.:
  IPv6 Prefix     : 2001:1::/64
    Flags : Up Internal Metric : 10
  IPv6 Prefix     : 3001:1::/64
    Flags : Up Internal Metric : 10
  IPv6 Prefix     : 4001:1::/64
    Flags : Up Internal Metric : 10
TE IP Reach.:
  IPv4 Prefix     : 11.1.1.0/24 (Dir.:Up) Metric : 10
  IPv4 Prefix     : 22.1.1.0/24 (Dir.:Up) Metric : 10
  IPv4 Prefix     : 21.1.1.0/24 (Dir.:Up) Metric : 10
  IPv4 Prefix     : 10.135.38.0/24 (Dir.:Up) Metric : 1

level-1 LSP count : 1

Displaying level-2 database

------------------------------------------------------------------
LSP ID        : 1720.2116.0051.00-00             Level     : L2
Sequence      : 0x45       Checksum  : 0xb465    Lifetime  : 981
Version       : 1          Pkt Type  : 20        Pkt Ver   : 1
Attributes    : L1L2       Max Area  : 3
SysID Len     : 6          Used Len  : 635       Alloc Len : 1489
TLVs   :
  Area Addresses   :
    Area Address   : (3) 49.0000
  Supp protocols   :
    Protocols      : Ipv4  Ipv6
  IS-Hostname      :
    Hostname       : HostA
  IS Neighbors     :
    Virtual Flag   : 0
    Neighbor       : 1720.2116.0052.00 Metric : 10 (I)
IPv4 I/F Address :
  IP Address       : 172.21.160.51
  IP Address       : 172.21.160.52
IPv6 I/F Address :
  IPv6 Address     : 2001:1::1
  IPv6 Address     : 3001:1::1
IPv4 Internal Reach:
  IP Prefix       : 16.16.16.0/24 (Dir.: UP ) Metric  : 10 (I)
  IP Prefix       : 17.17.17.0/24 (Dir.: UP ) Metric  : 10 (I)
IPv4 External Reach:
  IP Prefix       : 24.24.24.0/24 (Dir.: UP ) Metric  : 10 (E)
  IP Prefix       : 25.25.25.0/24 (Dir.: UP ) Metric  : 10 (E)
IPv6 Reach.:
  IPv6 Prefix     : 3001:1::/64
    Flags : Up Internal Metric : 10
TE IP Reach.:
  IPv4 Prefix     : 21.1.1.0/24 (Dir.:Up) Metric : 10
  IPv4 Prefix     : 10.135.38.0/24 (Dir.:Up) Metric : 1
  IPv4 Prefix     : 11.1.1.0/24 (Dir.:Up) Metric : 1

level-2 LSP count : 1

================================================================================
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP ID</td>
<td>The LSP ID. Indicates the system ID and the pseudo-node ID of the originating router.</td>
</tr>
<tr>
<td>Sequence</td>
<td>The sequence number of the LSP. The Sequence number is a value used to identify old and duplicate LSPs.</td>
</tr>
<tr>
<td>Checksum</td>
<td>The checksum value of the LSP.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The number of seconds the LSP remains valid. The LSP lifetime value of zero indicates that this LSP is being removed from the Link State Database of all the routers.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the IS-IS protocol that has generated the LSP.</td>
</tr>
<tr>
<td>Pkt Type</td>
<td>The IS-IS PDU type number derived from the PDU header, which can be 18 or 20. The number 18 represents L1 LSP PDU type and 20 represents L2 LSP PDU type.</td>
</tr>
<tr>
<td>Pkt Ver</td>
<td>The version of the IS-IS protocol that has generated the packet.</td>
</tr>
<tr>
<td>Attributes</td>
<td>The level capability of the router.</td>
</tr>
<tr>
<td>Max Area</td>
<td>The Maximum number of areas supported by the originating router of the LSP.</td>
</tr>
<tr>
<td>SysID Len</td>
<td>The length of the system-id as used by the originating router.</td>
</tr>
<tr>
<td>Used Len</td>
<td>The length used by the LSP.</td>
</tr>
<tr>
<td>Alloc Len</td>
<td>The length allocated for the LSP to be stored.</td>
</tr>
<tr>
<td>Area Address</td>
<td>The area ID of the router.</td>
</tr>
<tr>
<td>Supp protocols</td>
<td>The network layer protocols that are supported.</td>
</tr>
<tr>
<td>IS-Host Name</td>
<td>The host name of the router.</td>
</tr>
<tr>
<td>System ID</td>
<td>The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.</td>
</tr>
<tr>
<td>IS Neighbors</td>
<td>The list of reachable IS-IS neighbors.</td>
</tr>
<tr>
<td>IPv4 Internal Reach</td>
<td>The list of IS-IS internal routes.</td>
</tr>
<tr>
<td>IPv6 Reach</td>
<td>The list of IS-IS IPv6 internal routes.</td>
</tr>
<tr>
<td>IP Prefix</td>
<td>The IP address and subnet mask of the destination.</td>
</tr>
<tr>
<td>Metrics</td>
<td>The metric value to reach the destination.</td>
</tr>
<tr>
<td>IPv4 External Reach</td>
<td>The list of external IS-IS routes.</td>
</tr>
<tr>
<td>IPv6 Reach</td>
<td>The list of external IS-IS IPv6 routes.</td>
</tr>
<tr>
<td>level-1 LSP Count</td>
<td>The number of Level-1 LSPs.</td>
</tr>
<tr>
<td>level-2 LSP Count</td>
<td>The number of Level-2 LSPs.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command was introduced.
Related Commands

**show ip isis hostname**
Displays the database of IS-IS host name and its corresponding system ID.

**clear ip isis lsp-database**
Clears and resets the IS-IS LSP database information.

MIB Objects

vRtrIsisLSPTable
 vRtrIsisLSPId
 vRtrIsisLSPSeq
 vRtrIsisLSPChecksum
 vRtrIsisLSPLifetimeRemain
 vRtrIsisLSPAttributes
 vRtrisisLSPVersion
 vRtrIsisLSPPktType
 vRtrIsisLSPSysIdLen
 vRtrIsisLSPAllocLen
 vRtrIsisLSPMaxArea
 vRtrIsisLSPBuff
 vRtrisisLSPUsedLen
show ip isis hostname

Displays the database of IS-IS host name and its corresponding system ID.

Syntax Definitions
N/A

Defaults
N/A

 Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples
-> show ip isis hostname
Hosts
========================================================================
<table>
<thead>
<tr>
<th>System Id</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800.0000.0002</td>
<td>core_west</td>
</tr>
<tr>
<td>1800.0000.0005</td>
<td>core_east</td>
</tr>
<tr>
<td>1800.0000.0008</td>
<td>asbr_west</td>
</tr>
<tr>
<td>1800.0000.0009</td>
<td>asbr_east</td>
</tr>
<tr>
<td>1800.0000.0010</td>
<td>abr_sjc</td>
</tr>
<tr>
<td>1800.0000.0011</td>
<td>abr_lax</td>
</tr>
<tr>
<td>1800.0000.0012</td>
<td>abr_nyc</td>
</tr>
<tr>
<td>1800.0000.0013</td>
<td>abr_dfw</td>
</tr>
<tr>
<td>1800.0000.0015</td>
<td>dist_oak</td>
</tr>
<tr>
<td>1800.0000.0018</td>
<td>dist_nj</td>
</tr>
<tr>
<td>1800.0000.0020</td>
<td>acc_nj</td>
</tr>
<tr>
<td>1800.0000.0021</td>
<td>acc_ri</td>
</tr>
<tr>
<td>1800.0000.0027</td>
<td>dist_arl</td>
</tr>
<tr>
<td>1800.0000.0028</td>
<td>dist_msq</td>
</tr>
<tr>
<td>1800.0000.0029</td>
<td>acc_arl</td>
</tr>
</tbody>
</table>
output definitions

| System Id | The system ID of the router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-Octet hexadecimal system ID. |
| Hostname  | The host name of the router. |

Release History

Release 7.3.3; command was introduced.

Related Commands

- **show ip isis adjacency** Displays information about IS-IS adjacent routers.
- **show ip isis database** Displays IS-IS LSP database information of the adjacent routers.
- **ip isis area-id** Configures the area ID for the router.

MIB Objects

- **vRtrIsisHostnameTable**
  - **vRtrIsisSysID**
  - **vRtrIsisHostname**
**show ip isis routes**

Displays the IS-IS route information from the routing table.

**show ip isis routes**

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
</tr>
<tr>
<td>6465</td>
</tr>
<tr>
<td>6560</td>
</tr>
<tr>
<td>6570M</td>
</tr>
<tr>
<td>6860</td>
</tr>
<tr>
<td>6860N</td>
</tr>
<tr>
<td>6865</td>
</tr>
<tr>
<td>6900</td>
</tr>
<tr>
<td>6900 V72/C32</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
</tr>
<tr>
<td>6900 C32E/T24C2/</td>
</tr>
<tr>
<td>6900 X24C2</td>
</tr>
<tr>
<td>9900</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Output</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 C32E/T24C2/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> show ip isis routes

```
----------------------------------------------------------------------------------
ISIS Routes
----------------------------------------------------------------------------------
Prefix          Metric  Lvl/Type  SPF-num  Nexthop       System ID
----------------------------------------------------------------------------------
1.1.1.0/24      10       1/Int     7        0.0.0.0       1720.2116.0051
2.2.2.0/24      10       1/Int     1        0.0.0.0       1720.2116.0051
3.3.3.0/24      10       1/Int     1        0.0.0.0       1720.2116.0051
4.4.4.0/24      10       1/Int     1        0.0.0.0       1720.2116.0051
5.5.5.0/24      10       1/Int     1        0.0.0.0       1720.2116.0051
6.6.6.0/24      10       1/Int     1        0.0.0.0       1720.2116.0051
----------------------------------------------------------------------------------
Routes : 8
```

**output definitions**

- **Prefix**: The IP prefix and mask of the destination routes.
- **Metric**: The cost to reach the destination route.
- **Lvl/Type**: The level and route type of the routes.
**output definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF-num</td>
<td>The version of the SPF calculation used to select the route.</td>
</tr>
<tr>
<td>Nexthop</td>
<td>The Next Hop address to reach the destination.</td>
</tr>
<tr>
<td>System ID</td>
<td>The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- `show ip isis adjacency` Displays information about IS-IS adjacent routers.
- `show ip isis database` Displays IS-IS LSP database information of the adjacent routers.

**MIB Objects**

`vRtrisisRouteTable`
  - `vRtrisisRouteLevel`
  - `vRtrisisRouteSpfVersion`
  - `vRtrisisRouteType`
  - `vRtrisisRouteDest`
  - `vRtrisisRouteNexthopIP`
  - `vRtrisisRouteNexthopSysID`
  - `vRtrisisRouteMetric`
  - `vRtrisisRouteMask`
show ip isis routes6

Displays the IS-IS IPv6 route information from the routing table.

show ip isis routes6

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ip isis routes6

ISISv6 Routes

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Metric</th>
<th>Lvl/Type</th>
<th>Vlan-Id</th>
<th>Nexthop</th>
<th>System ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001::/64</td>
<td>10</td>
<td>1/Int</td>
<td>6</td>
<td>::</td>
<td>0300.0100.1001</td>
</tr>
<tr>
<td>3001::/64</td>
<td>10</td>
<td>1/Int</td>
<td>11</td>
<td>::</td>
<td>0300.0100.1001</td>
</tr>
<tr>
<td>4001::/64</td>
<td>10</td>
<td>1/Int</td>
<td>6</td>
<td>::</td>
<td>0300.0100.1001</td>
</tr>
<tr>
<td>5001::/64</td>
<td>20</td>
<td>1/Int</td>
<td>6</td>
<td>fe80::213:c3ff:fe9a:2761</td>
<td>0000.0000.0001</td>
</tr>
</tbody>
</table>

Routes : 4

output definitions

Prefix: The IP prefix and mask of the IPv6 destination routes.
Metric: The cost to reach the destination route.
Lvl/Type: The level and route type of the routes.
SPF-num: The version of the SPF calculation used to select the route.
**output definitions**

- **NextHop**: The Next Hop address to reach the destination.
- **System ID**: The system ID of the adjacent router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- `show ip isis adjacency`: Displays information about IS-IS adjacent routers.
- `show ip isis database`: Displays IS-IS LSP database information of the adjacent routers.

**MIB Objects**

- **N/A**
**show ip isis spf**

Displays the IS-IS SPF calculation information.

`show ip isis spf [detail]`

### Syntax Definitions

- **detail**: Indicates that the output is displayed in a detailed manner.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The SPF path table is common for both IPv4 and IPv6.

### Examples

```
-> show ip isis spf
---------------------------------------------------------------------------------------------
ISIS Path Table
---------------------------------------------------------------------------------------------
Node        VlanId        Nexthop
---------------------------------------------------------------------------------------------
0000.0000.0001.00  6    0000.0000.0001
---------------------------------------------------------------------------------------------
SPF count: 1
---------------------------------------------------------------------------------------------
```

**output definitions**

- **Node**: The system ID of the routers.
- **VlanId**: The VLAN ID.
- **Nexthop**: The system ID of the Next Hop router.
-> show ip isis spf detail

IS-IS Path Table

Node : 0000.0000.0001.00   Metric : 10
VlanId : 6   SNPA : None
Nexthop : 0000.0000.0001

SPF count: 1

Output Definitions

<table>
<thead>
<tr>
<th>Node</th>
<th>The system ID of the routers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric</td>
<td>The metric value used for SPF calculations.</td>
</tr>
<tr>
<td>VlanID</td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>SNPA</td>
<td>The SNPA address of the router.</td>
</tr>
<tr>
<td>Nexthop</td>
<td>The system ID of the Next Hop router.</td>
</tr>
<tr>
<td>SPF count</td>
<td>The number of SPF calculations done by the router.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis spf-log  Displays the IS-IS SPF log.
show ip isis status  Displays the IS-IS status.

MIB Objects

vRtrIsisPathTable
  vRtrIsisPathID
  vRtrIsisPathIfIndex
  vRtrIsisPathNHopSysID
  vRtrIsisPathMetric
  vRtrIsisPathSNPA
show ip isis spf-log

Displays the IS-IS SPF log.

show ip isis spf-log [detail]

Syntax Definitions

detail Indicates that the output is displayed in a detailed manner.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays the last 20 IS-IS SPF events.

Examples

-> show ip isis spf-log

IS-IS SPFLog

When   Duration   L1-Nodes   L2-Nodes   Event-Count
01/30/2005 11:01:54 <0.01s 1 1 3

Log Entries : 1

output definitions

When The date on which the SPF calculation was completed.
Duration The time duration of the event.
L1-Nodes The number of Level-1 nodes.
L2-Nodes The number of Level-2 nodes.
Event-Count The number of SPF calculations.
Log Entries The total number of log entries.
-> show ip isis spf-log detail
=============================================================================
ISIS SPFLog
=============================================================================
SpfTimeStamp : SUN OCT 01 05:15:29 2006
spfRunTime : 0
Spf Involved L1 Nodes : 69
Spf Involved L2 Nodes : 71
Spf Event-count : 169
Last TriggeredLspId : 0020.0200.2001.00-4a
Spf Trigger Reason : newAdjacency(0) ,lspExpired(8) ,lspChanged(10)
SpfTimeStamp : SUN OCT 01 05:15:46 2006
spfRunTime : 0
Spf Involved L1 Nodes : 72
Spf Involved L2 Nodes : 72
Spf Event-count : 227
Last TriggeredLspId : 0020.0200.2001.00-4a
Spf Trigger Reason : newAdjacency(0) ,lspExpired(8) ,lspChanged(10)
=============================================================================
Log Entries : 2
=============================================================================

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpfTimeStamp</td>
<td>The timestamp when the SPF run started on the system.</td>
</tr>
<tr>
<td>spfRunTime</td>
<td>The time (in hundredths of a second) required to complete the SPF run.</td>
</tr>
<tr>
<td>Spf Involved L1 Nodes</td>
<td>The number of Level-1 nodes involved in the SPF calculation.</td>
</tr>
<tr>
<td>Spf Involved L2 Nodes</td>
<td>The number of Level-2 nodes involved in the SPF calculation.</td>
</tr>
<tr>
<td>Spf Event-count</td>
<td>The number of SPF events that triggered the SPF calculation.</td>
</tr>
<tr>
<td>Last TriggeredLspId</td>
<td>The LSP ID of the last LSP processed before the SPF run.</td>
</tr>
<tr>
<td>Spf trigger Reason</td>
<td>Indicates the reasons (newAdjacency, lspExpired, or lspChanged) for SPF calculations.</td>
</tr>
<tr>
<td>Log Entries</td>
<td>The number of SPF logs.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis spf Displays the IS-IS SPF calculation information.
clear ip isis spf-log Clears and resets the IS-IS SPF log information.

MIB Objects

vRtrIsisSpfLogTable
  vRtrIsisSpfRunTime
  vRtrIsisSpfL1Nodes
  vRtrIsisSpfL2Nodes
  vRtrIsisSpfEventCount
  vRtrIsisSpfLastTriggerLSPId
  vRtrIsisSpfTriggerReason
show ip isis statistics

Displays the IS-IS statistics information.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ip isis statistics
```

```
ISIS Statistics

ISIS Instance : 1 SPF Runs : 44
Purge Initiated : 0 LSP Regens : 54

CSPF Statistics
Requests : 0 Request Drops : 0
Paths Found : 0 Paths Not Found : 0

PDU Type Received Processed Dropped Sent Retransmitted
LSP 185 184 1 54 0
IIH 8382 8382 0 2796 0
CSNP 3352 352 0 0 0
PSNP 0 0 0 4 0
Unknown 0 0 0 0 0
```
**output definitions**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ISIS Instance</strong></td>
<td>The number of IS-IS instances.</td>
</tr>
<tr>
<td><strong>SPF Runs</strong></td>
<td>The number of SPF calculations that have been performed.</td>
</tr>
<tr>
<td><strong>Purge Initiated</strong></td>
<td>The number of purges that the system initiated. A purge is initiated if the router decides that a link-state PDU must be removed from the database.</td>
</tr>
<tr>
<td><strong>LSP Regens</strong></td>
<td>The number of LSPs that have been regenerated. An LSP is regenerated when it nears the end of its lifetime and has not changed.</td>
</tr>
<tr>
<td><strong>Requests</strong></td>
<td>The number of CSNP requests received.</td>
</tr>
<tr>
<td><strong>Request Drops</strong></td>
<td>The number of CSNP requests that are dropped.</td>
</tr>
<tr>
<td><strong>Paths Found</strong></td>
<td>The number of paths found.</td>
</tr>
<tr>
<td><strong>Paths Not Found</strong></td>
<td>The number of paths not found.</td>
</tr>
<tr>
<td><strong>PDU Type</strong></td>
<td>The type of PDU.</td>
</tr>
<tr>
<td><strong>Received</strong></td>
<td>The number of PDUs received since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Processed</strong></td>
<td>The number of PDUs that are processed (number of PDUs received less the number dropped).</td>
</tr>
<tr>
<td><strong>Dropped</strong></td>
<td>The number of PDUs that are dropped.</td>
</tr>
<tr>
<td><strong>Sent</strong></td>
<td>The number of PDUs transmitted since IS-IS started or since the statistics were set to zero.</td>
</tr>
<tr>
<td><strong>Retransmitted</strong></td>
<td>The number of PDUs that are retransmitted.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

*clear ip isis statistics* Clears and resets the IS-IS statistics information.
### MIB Objects

- **vRtrIisisStatsTable**
  - vRtrIisisSpfRuns
  - vRtrIisisLSPRegenerations
  - vRtrIisisInitiatedPurges
  - vRtrIisisLSPRecd
  - vRtrIisisLSPDrop
  - vRtrIisisLSPSent
  - vRtrIisisLSPRetrans
  - vRtrIisisIIHRecd
  - vRtrIisisIIHDrop
  - vRtrIisisIIHSent
  - vRtrIisisIIHRetrans
  - vRtrIisisCSNPRecd
  - vRtrIisisCSNPDrop
  - vRtrIisisCSNPSent
  - vRtrIisisCSNPRetrans
  - vRtrIisisPSNPRecd
  - vRtrIisisPSNPDrop
  - vRtrIisisPSNPSent
  - vRtrIisisPSNPRetrans
  - vRtrIisisUnknownRecd
  - vRtrIisisUnknownDrop
  - vRtrIisisUnknownSent
  - vRtrIisisUnknownRetrans
  - vRtrIisisCSPFRequests
  - vRtrIisisCSPFDroppedRequests
  - vRtrIisisCSPPPathsFound
  - vRtrIisisCSPPPathsNotFound
**show ip isis status**

Displays the IS-IS status.

```
show ip isis status
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show ip isis status
```

```
ISIS Status
System Id : 2cf.a213.e402
Admin State : DOWN
Protocols Enabled : IPv4 IPv6
Last Enabled : Mon Oct 30 06:58:41 2017
Level Capability : L1L2
Authentication Check : True
Authentication Type : None
Graceful Restart : Disabled
GR helper-mode : Disabled
LSP Lifetime : 1200
LSP Wait : Max: 5 sec Initial: 0 sec Second: 1 sec
Adjacency Check : Loose
L1 Auth Type : None
L2 Auth Type : None
L1 Wide Metrics-only : Disabled
L2 Wide Metrics-only : Disabled
L1 LSDB Overload : Disabled
L2 LSDB Overload : Disabled
L1 LSPs : 0
```
L2 LSPs : 0
Last SPF : Mon Oct 30 06:58:41 2017
SPF Wait : Max: 10000 ms Initial: 1000 ms Second: 1000 ms
Hello-Auth Check : Enabled
Csnp-Auth Check : Enabled
Psnp-Auth Check : Enabled
L1 Hello-Auth Check : Enabled
L1 Csnp-Auth Check : Enabled
L1 Psnp-Auth Check : Enabled
L2 Hello-Auth Check : Enabled
L2 Csnp-Auth Check : Enabled
L2 Psnp-Auth Check : Enabled
Multi-Topology : Disabled
Auto-Configuration : Disabled
Area Address : None
BFD Status : Disabled

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>The system ID of the router. The system ID is a fixed size, six octet field in the NSAP. In an IS-IS routing domain, each router is identified by a 6-octet hexadecimal system ID.</td>
</tr>
<tr>
<td>Admin State</td>
<td>The state of the router (Up or Down).</td>
</tr>
<tr>
<td>Protocols Enabled</td>
<td>The protocol enabled on the router: IPv4 or IPv6</td>
</tr>
<tr>
<td>Last Enabled</td>
<td>The date and time when the router is enabled.</td>
</tr>
<tr>
<td>Level Capability</td>
<td>The level capability of the router (L1, L2, or L1L2).</td>
</tr>
<tr>
<td>Authentication Check</td>
<td>Indicates the status of the authentication (true or false).</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The type of authentication (simple, md5, keychain, none).</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Indicates if graceful restart is Enabled or Disabled.</td>
</tr>
<tr>
<td>GR helper-mode</td>
<td>Indicates if the helper mode of graceful restart is Enabled or Disabled.</td>
</tr>
<tr>
<td>LSP Lifetime</td>
<td>The Lifetime of the LSP (in seconds).</td>
</tr>
<tr>
<td>LSP Wait</td>
<td>The Wait time of the LSP (in seconds).</td>
</tr>
<tr>
<td>Adjacency Check</td>
<td>The adjacency check configuration on the router</td>
</tr>
<tr>
<td>L1 Auth Type</td>
<td>The authentication type (simple, md5, keychain, none) for Level-1 adjacency.</td>
</tr>
<tr>
<td>L2 Auth Type</td>
<td>The authentication type (simple, md5, keychain, none) for Level-2 adjacency.</td>
</tr>
<tr>
<td>L1 Wide Metrics-only</td>
<td>Indicates whether wide metrics is Enabled or Disabled for Level-1 adjacency.</td>
</tr>
<tr>
<td>L2 Wide Metrics-only</td>
<td>Indicates whether wide metrics is Enabled or Disabled for Level-2 adjacency.</td>
</tr>
<tr>
<td>L1 LSDB Overload</td>
<td>Indicates whether LSDB Overload is Enabled or Disabled for Level-1 adjacency.</td>
</tr>
<tr>
<td>L2 LSDB Overload</td>
<td>Indicates whether LSDB Overload is Enabled or Disabled for Level-2 adjacency.</td>
</tr>
<tr>
<td>L1 LSPs</td>
<td>The number of LSPs for Level-1 adjacency.</td>
</tr>
<tr>
<td>L2 LSPs</td>
<td>The number of LSPs for Level-2 adjacency.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last SPF</td>
<td>The date and duration of the last SPF calculation.</td>
</tr>
<tr>
<td>SPF Wait</td>
<td>The Wait time for the SPF calculation.</td>
</tr>
<tr>
<td>Hello-Auth Check</td>
<td>Indicates the status of global Hello authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>Csnp-Auth Check</td>
<td>Indicates the status of global CSNP authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>Psnp-Auth Check</td>
<td>Indicates the status of global PSNP authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>L1 Hello-Auth Check</td>
<td>Indicates the status of L1 Hello authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>L1 Csnp-Auth Check</td>
<td>Indicates the status of L1 CSNP authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>L1 Psnp-Auth Check</td>
<td>Indicates the status of L1 PSNP authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>L2 Hello-Auth Check</td>
<td>Indicates the status of L2 Hello authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>L2 Csnp-Auth Check</td>
<td>Indicates the status of L2 CSNP authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>L2 Psnp-Auth Check</td>
<td>Indicates the status of L2 PSNP authentication check (Enabled or Disabled).</td>
</tr>
<tr>
<td>Auto-Configuration</td>
<td>Indicates the status of auto-configuration for ISIS. (Enabled or Disabled)</td>
</tr>
<tr>
<td>Area Address</td>
<td>The area address of the router.</td>
</tr>
<tr>
<td>BFD Status</td>
<td>Indicates the status of IS-IS registration with BFD. (Enabled or Disabled)</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command introduced.
Release 7.3.4; Auto-Configuration field added.
Release 8.4.1.R03; BFD Status field added.

Related Commands

show ip isis statistics Displays statistics for the IS-IS configuration.
MIB Objects

vRtrIsisTable
  vRtrIsisLastEnabledTime
  vRtrIsisAuthKey
  vRtrIsisAuthType
  vRtrIsisLspLifetime
  vRtrIsisOverloadTimeout
  vRtrIsisLastSpfRun
  vRtrIsisGracefulRestart
  vRtrIsisOverloadOnBootv
  vRtrIsisOverloadOnBootimeout
  vRtrIsisSpfWait
  vRtrIsisSpfInitialWait
  vRtrIsisSpfSecondWait
  vRtrIsisLspMaxWait
  vRtrIsisLspInitialWait
  vRtrIsisLspSecondWait
  vRtrIsisCsnpAuthentication
  vRtrIsisHelloAuthentication
  vRtrIsisPsnpAuthentication
  vRtrIsisGRHelperMode
  vRtrIsisSpfWait
  vRtrIsisMTEnabled

vRtrIsisLevelTable
  vRtrIsisLevelAuthKey
  vRtrIsisLevelAuthType
  vRtrIsisLevelExtPreference
  vRtrIsisLevelPreference
  vRtrIsisLevelWideMetricsOnly
  vRtrIsisLevelCsnpAuthentication
  vRtrIsisLevelPsnpAuthentication
  vRtrIsisLevelHelloAuthentication
  vRtrIsisLevelWideMertic
  vRtrIsisLevelNumLSPs
show ip isis summary-address

Displays the IS-IS summary address database.

show ip isis summary-address [ip_address [mask]]

Syntax Definitions

ip_address The 32-bit IP address.

/mask The netmask value. The valid range is 1–32.

Defaults

By default summary address information for all the IP addresses is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the ip_address parameter with this command to view the summary address information for a specific IP address.

Examples

-> show ip isis summary-address
=======================================
ISIS Summary Address
=======================================
Address                     Level
---------------------------------------
1.0.0.0/8                   L1
2.1.0.0/24                  L1L2
3.1.2.3/32                  L2
---------------------------------------
Summary Address : 3
=======================================

output definitions

| Address | The summary address for a range of IPv4 addresses. |
| Level   | The capability level of the router.             |
| Summary Address | The number of summarized addresses. |
**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

*ip isis summary-address*  
Adds or deletes the summary address.

**MIB Objects**

`vRtrIsissummaryTable`
- `vRtrIsisSummPefix`
- `vRtrIsisSummMask`
- `vRtrIsisSummLevel`
**show ip isis vlan**

Displays the IS-IS IPv4 and IPv6 interface information on a VLAN in the IS-IS database.

**show ip isis vlan [vlan_id] [detail]**

---

**Syntax Definitions**

- **vlan_id**
  - The VLAN ID.
- **detail**
  - Indicates that the output is displayed in a detailed manner.

---

**Defaults**

By default, the interface information for all the interfaces is displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the `vlan_id` parameter with this command to view information for a specific VLAN.

---

**Examples**

```
-> show ip isis vlan

ISIS VLan
-----------------------------------------------
Interface Address-family Level VlanID Oper-state Admin-state L1/L2-Metric
-----------------------------------------------
  ospf    ipv4 L1L2 1l DOWN  UP  10/10
  vlan11  ipv6 L1L2 1l DOWN  UP  10/10
-----------------------------------------------
Vlans : 2
-----------------------------------------------
```

---

**output definitions**

- **Interface**
  - The name of the IS-IS interface.
- **Address-family**
  - The address family extension: IPv4 or IPv6
- **Level**
  - The level capability of the interface.
- **VlanID**
  - The VLAN ID of the interface.
- **Oper-state**
  - The operational state of the interface (`up` or `down`).
output definitions

**Admin-state**
The administrative state of the interface (**up** or **down**).

**L1/L2-Metric**
The metric value of the router for the corresponding capability level.

**Vlans**
The total number of VLANS.

```
-> show ip isis vlan detail
```

```
ISIS Interface

VlanId             : 10             Level Capability  : L1L2
Oper State         : Up             Admin State       : Up
Auth Type          : Keychain(3)    Address Families  : IPv4, IPv6
Circuit Id         : 1              RetransmitInt     : 5
Type               : Broadcast      LSP Pacing Int    : 100
Mesh Group         : Inactive       CSNP Int          : 10
BFD Status         : Disabled

Level              : 1              Adjacencies       : 0
Desg IS            : abr_nyc
Auth Type          : None           Metric            : 10
Hello Timer        : 9               Hello Mult       : 3
Priority           : 64              Passive           : No
Level              : 2              Adjacencies : 0
Desg IS            : abr_nyc
Auth Type          : None            Metric           : 10
Hello Timer        : 9               Hello Mult       : 3
Priority           : 64              Passive          : No

VlanId             : 20              Level Capability : L1L2
Oper State         : Up             Admin State : Up
Auth Type          : None            Address Families : IPv4, IPv6
Circuit Id         : 8               RetransmitInt    : 5
Type               : Pt-to-Pt      LSP Pacing Int : 100
Mesh Group         : Inactive       CSNP Int         : 10
BFD Status         : Disabled

Level              : Pt-to-Pt
Desg IS            : abr_nyc
Auth Type          : None            Metric           : 10
Hello Timer        : 9               Hello Mult       : 3
Priority           : 64              Passive          : No
```

vlans : 2

```
output definitions

**VlanId**
The VLAN ID.

**Level Capability**
The level capability of the interface.

**Oper State**
The operational state of the interface (**up** or **down**).

**Admin State**
The administrative state of the interface (**up** or **down**).

**Auth Type**
Indicates the authentication type (**simple**, **MD5**, **keychain**, **none**) of the interface.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Families</td>
<td>The address family extension: IPv4 or IPv6</td>
</tr>
<tr>
<td>Circuit Id</td>
<td>The circuit ID of the interface.</td>
</tr>
<tr>
<td>RetransmitInt</td>
<td>Specifies the minimal interval of time, in seconds, between retransmission of an LSP on the point-to-point interface.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of interface: <strong>Broadcast</strong> or <strong>Pt-to-Pt</strong> (point to point).</td>
</tr>
<tr>
<td>LSP Pacing Int</td>
<td>The LSP Pacing interval.</td>
</tr>
<tr>
<td>Mesh Group</td>
<td>The status of the mesh group (<strong>Active</strong> or <strong>Inactive</strong>).</td>
</tr>
<tr>
<td>BFD Status</td>
<td>The status of BFD on the IS-IS VLAN interface (<strong>Enabled</strong> or <strong>Disabled</strong>).</td>
</tr>
<tr>
<td>CSNP Int</td>
<td>The CSNP interval.</td>
</tr>
<tr>
<td>Level</td>
<td>Indicates the IS-IS level of the neighbor (<strong>L1</strong>, <strong>L2</strong>, or <strong>L1L2</strong>).</td>
</tr>
<tr>
<td>Adjacencies</td>
<td>The number of adjacencies formed.</td>
</tr>
<tr>
<td>Desg IS</td>
<td>The ID of the LAN Designated Intermediate System on this circuit at this level.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Indicates the authentication type (<strong>simple</strong>, <strong>MD5</strong>, <strong>keychain</strong>, <strong>none</strong>) for the specified level.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric value of this circuit for a specific level.</td>
</tr>
<tr>
<td>Hello Timer</td>
<td>Indicates the Hello timer value.</td>
</tr>
<tr>
<td>Hello Mult</td>
<td>Indicates the Hello multiplier value.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority value of the interface.</td>
</tr>
<tr>
<td>Passive</td>
<td>Indicates whether the interface is configured as a passive interface (<strong>Yes</strong> or <strong>No</strong>).</td>
</tr>
<tr>
<td>Vlans</td>
<td>The total number of VLANs.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- **ip isis vlan** Configures IPv4 or IPv6 IS-IS circuit on a particular VLAN.
MIB Objects

isisCircTable
  isisCircLocalID
  isisCircAdminState
  isisCircType
  isisCircLevel
  isisCircPassiveCircuit
  isisCircMeshGroup

isisCircLevelTable
  isisCircLevelISPriority
  isisCircLevelCircID
  isisCircLevelDesIS
  isisCircLevelHelloMultiplier
  isisCircLevelHelloTimer
  isisCircLevelCSNPInterval

vRtrIsisIfTable
  vRtrIsisIfAdminState
  vRtrIsisIfOperState
  vRtrIsisIfCSnpInterval
  vRtrIsisIfHelloAuthKey
  vRtrIsisIfHelloAuthType
  vRtrIsisIfLspPacingInterval
  vRtrIsisIfRetransmitInterval
  vRtrIsisIfHelloAuthKeyChainId

vRtrIsisIfLevelTable
  vRtrIsisIfLevelHelloAuthKey
  vRtrIsisIfLevelHelloAuthType
  vRtrIsisIfLevelPassive
  vRtrIsisIfLevelNumAdjacencies
  vRtrIsisIfLevelISPriority
  vRtrIsisIfLevelHelloTimer
  vRtrIsisIfLevelOperMetric
  vRtrIsisIfLevelAdminMetric
  vRtrIsisIfLevelHelloAuthKeyChainId
show ip isis summary-address6

Displays the IS-IS IPv6 summary address database.

show ip isis summary-address6 [ip_address [/mask]]

**Syntax Definitions**

- **ip_address**
  - The 32-bit IP address.
- **/mask**
  - The netmask value. The valid range is 1–32.

**Defaults**

By default, summary address information for all the IP addresses is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **ip_address** parameter with this command to view the summary address information for a specific IP address.

**Examples**

```
-> show ip isis summary-address6
==========================================================================
ISISv6 Summary Address
==========================================================================
Address Level
==========================================================================
1111:1::/64 L1
==========================================================================
Summary Address : 1
```

**output definitions**

- **Address**
  - The summary address for a range of IPv6 addresses.
- **Level**
  - The capability level of the router.
- **Summary Address**
  - The number of summarized addresses.
Release History

Release 7.3.3; command was introduced.

Related Commands

ip isis summary-address6  Configures the IPv6 summary address.

MIB Objects

N/A
clear ip isis adjacency

Clears and resets the IS-IS adjacency database information.

`clear ip isis adjacency [system-id nbr_sys_id]`

**Syntax Definitions**

`nbr_sys_id` The system ID of the neighbor router.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the `nbr_sys_id` parameter is specified, only the entries specific to that system ID are removed from the database.

**Examples**

`-> clear ip isis adjacency system-id 1122.3344.5566`

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

`show ip isis adjacency` Displays information about IS-IS adjacent routers.
**MIB Objects**

isisISAdjTable
- isisISAdjIndex
- isisISAdjState
- isisISAdjNeighSNPAAddress
- isisISAdjNeighSysType
- isisISAdjNeighSysID
- isisISAdjUsage
- isisISAdjHoldTimer
- isisISAdjNeighPriority
- isisISAdjUpTime

vRtrIsisISAdjTable
- vRtrIsisISAdjExpiresIn
- vRtrIsisISAdjCircLevel
- vRtrIsisISAdjRestartSupport
- vRtrIsisISAdjRestartStatus
- vRtrIsisISAdjRestartSuppressed
clear ip isis lsp-database

Clears and resets the IS-IS LSP database information.

clear ip isis lsp-database [system-id sys_id]

---

**Syntax Definitions**

*sys_id*  
The system ID of the router.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

If the *sys_id* parameter is specified, only the entries specific to that system ID are removed from the database.

---

**Examples**

-> clear ip isis lsp-database system-id 000a.1234.2345

---

**Release History**

Release 7.3.3; command was introduced.

---

**Related Commands**

- **show ip isis database**  
  Displays IS-IS LSP database information of the adjacent routers.
**MIB Objects**

vRtrIsisLSPTable
  vRtrIsisLSPId
  vRtrIsisLSPSeq
  vRtrIsisLSPChecksum
  vRtrIsisLSPLifetimeRemain
  vRtrIsisLSPVersion
  vRtrIsisLSPPktType
  vRtrIsisLSPPktVersion
  vRtrIsisLSPMaxArea
  vRtrIsisLSPSysIdLen
  vRtrIsisLSPAtributes
  vRtrIsisLSPUsedLen
  vRtrIsisLSPAlocLen
  vRtrIsisLSPBuff
  vRtrIsisLSPZeroRLT
clear ip isis spf-log

Clears and resets the IS-IS SPF log information.

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples

-> clear ip isis spf-log

Release History
Release 7.3.3; command was introduced.

Related Commands

show ip isis spf-log Displays the IS-IS SPF log.

MIB Objects

vrtrIsisSpfLogTable
  vrtrIsisSpfRunTime
  vrtrIsisSpfL1Nodes
  VRtrIsisSpfL2Nodes
  vRtrIsisSpfEventCount
  vrtrIsisSpfLastTriggerLSPId
  vRtrIsisSpfTriggerReason
clear ip isis statistics

Clears and resets the IS-IS statistics information.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> clear ip isis statistics

Release History

Release 7.3.3; command was introduced.

Related Commands

show ip isis statistics Displays the IS-IS statistics information.
MIB Objects

vRtrIisisStatsTable
  vRtrIisisSpfRuns
  vRtrIisisLSPRegenerations
  vRtrIisisInitiatedPurges
  vRtrIisisLSPRecd
  vRtrIisisLSPDrop
  vRtrIisisLSPSent
  vRtrIisisLSPRetrans
  vRtrIisisIIHRecd
  vRtrIisisIIHDrop
  vRtrIisisIIHSent
  vRtrIisisIIHRetrans
  vRtrIisisCSNPRecd
  vRtrIisisCSNPDrop
  vRtrIisisCSNPSent
  vRtrIisisCSNPRetrans
  vRtrIisisPSPRecd
  vRtrIisisPSNPDrop
  vRtrIisisPSNPSent
  vRtrIisisPSNPRetrans
  vRtrIisisUnknownRecd
  vRtrIisisUnknownDrop
  vRtrIisisUnknownSent
  vRtrIisisUnknownRetrans
  vRtrIisisCSPPRequests
  vRtrIisisCSPPDroppedRequests
  vRtrIisisCSPPPathsFound
  vRtrIisisCSPPPathsNotFound
ip isis multi-topology

Enables M-ISIS (multi-topology) capability support for IS-IS. If enabled, IPv6 SPF computation is performed separate from the IPv4 SPF computation.

ip isis multi-topology
no ip isis multi-topology

Syntax Definitions

N/A

Defaults

By default, multi-topology is disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Changing the multi-topology mode with this command results in internal disabling and re-enabling of the IS-IS protocol with the new mode of operation. This will cause IS-IS adjacencies to be reset.

Examples

-> ip isis multi-topology
-> no ip isis multi-topology

Release History

Release 7.3.4; command was introduced.

Related Commands

- show ip isis status Displays the IS-IS status.
- show ip isis adjacency Displays information about IS-IS adjacent routers.

MIB Objects

- vRtrIsisEntry
- vRtrIsisMTEncabled
This chapter describes the CLI commands used to configure the BGP (Border Gateway Protocol) and Multiprotocol extensions to BGP. BGP is a protocol for exchanging routing information between gateway hosts in a network of ASs (autonomous systems). BGP is the most common protocol used between gateway hosts on the Internet. The routing table exchanged contains a list of known routers, the addresses they can reach, and a preference metrics associated with the path to each router so that the best available route is chosen.

Multiprotocol Extensions to BGP-4 supports the exchange of IPv6 unicast prefixes, as well as the establishment of BGP peering sessions with BGP speakers identified by their IPv6 addresses.

The OmniSwitch implementation of BGP-4 and Multiprotocol Extensions to BGP-4 complies with the following RFCs: 4271, 2439, 3392, 2385, 1997, 4456, 3065, 4273, 4760, 2545, 7947.

**Note.** In the following document, the BGP terms “peer” and “neighbor” are used interchangeably to mean any BGP speaker known to the local router.

MIB information for BGP is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-VIRTUALROUTER-MIB.mib</td>
<td>alcatelIND1VirtualRouterMIB</td>
</tr>
<tr>
<td>ALCATEL-IND1-BGP-MIB.mib</td>
<td>alcatelIND1BGPMBIB</td>
</tr>
<tr>
<td>BGP4-MIB.mib</td>
<td>bgp</td>
</tr>
</tbody>
</table>
The following table summarizes the available commands:

<table>
<thead>
<tr>
<th>Global BGP Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ip load bgp</td>
<td></td>
</tr>
<tr>
<td>ip bgp admin-state</td>
<td></td>
</tr>
<tr>
<td>ip bgp autonomous-system</td>
<td></td>
</tr>
<tr>
<td>ip bgp bestpath as-path ignore</td>
<td></td>
</tr>
<tr>
<td>ip bgp cluster-id</td>
<td></td>
</tr>
<tr>
<td>ip bgp default local-preference</td>
<td></td>
</tr>
<tr>
<td>ip bgp fast-external-failover</td>
<td></td>
</tr>
<tr>
<td>ip bgp always-compare-med</td>
<td></td>
</tr>
<tr>
<td>ip bgp bestpath med missing-as-worst</td>
<td></td>
</tr>
<tr>
<td>ip bgp client-to-client reflection</td>
<td></td>
</tr>
<tr>
<td>ip bgp as-origin-interval</td>
<td></td>
</tr>
<tr>
<td>ip bgp synchronization</td>
<td></td>
</tr>
<tr>
<td>ip bgp confederation identifier</td>
<td></td>
</tr>
<tr>
<td>ip bgp maximum-paths</td>
<td></td>
</tr>
<tr>
<td>ip bgp log-neighbor-changes</td>
<td></td>
</tr>
<tr>
<td>ip bgp dampening</td>
<td></td>
</tr>
<tr>
<td>ip bgp dampening clear</td>
<td></td>
</tr>
<tr>
<td>ip bgp as-internal-format</td>
<td></td>
</tr>
<tr>
<td>ip bgp unicast</td>
<td></td>
</tr>
<tr>
<td>show ip bgp</td>
<td></td>
</tr>
<tr>
<td>show ip bgp statistics</td>
<td></td>
</tr>
<tr>
<td>show ip bgp dampening</td>
<td></td>
</tr>
<tr>
<td>show ip bgp dampening-stats</td>
<td></td>
</tr>
<tr>
<td>show ip bgp path</td>
<td></td>
</tr>
<tr>
<td>show ip bgp routes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Aggregate Configuration</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ip bgp aggregate-address admin-state</td>
<td></td>
</tr>
<tr>
<td>ip bgp aggregate-address as-set</td>
<td></td>
</tr>
<tr>
<td>ip bgp aggregate-address community</td>
<td></td>
</tr>
<tr>
<td>ip bgp aggregate-address local-preference</td>
<td></td>
</tr>
<tr>
<td>ip bgp aggregate-address metric</td>
<td></td>
</tr>
<tr>
<td>ip bgp aggregate-address summary-only</td>
<td></td>
</tr>
<tr>
<td>show ip bgp aggregate-address</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network (local route) Configurations</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ip bgp network</td>
<td></td>
</tr>
<tr>
<td>ip bgp network admin-state</td>
<td></td>
</tr>
<tr>
<td>ip bgp network community</td>
<td></td>
</tr>
<tr>
<td>ip bgp network local-preference</td>
<td></td>
</tr>
<tr>
<td>ip bgp network metric</td>
<td></td>
</tr>
<tr>
<td>show ip bgp network</td>
<td></td>
</tr>
</tbody>
</table>
### Neighbor (Peer) Configuration

- `ip bgp neighbor`
- `ip bgp neighbor ttl-security`
- `ip bgp neighbor activate-ipv4`
- `ip bgp neighbor activate-ipv6`
- `ip bgp neighbor ipv6-nexthop`
- `ip bgp neighbor admin-state`
- `ip bgp neighbor advertisement-interval`
- `ip bgp neighbor clear`
- `ip bgp neighbor route-reflector-client`
- `ip bgp neighbor default-originate`
- `ip bgp neighbor timers`
- `ip bgp neighbor conn-retry-interval`
- `ip bgp neighbor auto-restart`
- `ip bgp neighbor maximum-prefix`
- `ip bgp neighbor md5 key`
- `ip bgp neighbor ebgp-multihop`
- `ip bgp neighbor description`
- `ip bgp neighbor next-hop-self`
- `ip bgp neighbor passive`
- `ip bgp neighbor remote-as`
- `ip bgp neighbor remove-private-as`
- `ip bgp neighbor soft-reconfiguration`
- `ip bgp neighbor stats-clear`
- `ip bgp confederation neighbor`
- `ip bgp neighbor update-source`
- `ip bgp neighbor in-aspathlist`
- `ip bgp neighbor in-communitylist`
- `ip bgp neighbor in-prefixlist`
- `ip bgp neighbor out-aspathlist`
- `ip bgp neighbor out-communitylist`
- `ip bgp neighbor out-prefixlist`
- `ip bgp neighbor route-map`
- `ip bgp neighbor clear soft`
- `bgp neighbor check-first-as`
- `show ip bgp neighbors`
- `show ip bgp neighbors policy`
- `show ip bgp neighbors timer`
- `show ip bgp neighbors statistics`

### BGP BFD Commands

- `bgp neighbor check-first-as`
- `ip bgp bfd-state all-neighbors`
- `ip|ipv6 bgp neighbor bfd-state`
| Policy Commands | ip bgp policy aspath-list  
ip bgp policy aspath-list action  
ip bgp policy aspath-list priority  
ip bgp policy community-list  
ip bgp policy community-list action  
ip bgp policy community-list match-type  
ip bgp policy community-list priority  
ip bgp policy prefix-list  
ip bgp policy prefix-list action  
ip bgp policy prefix-list ge  
ip bgp policy prefix-list le  
ip bgp policy prefix6-list  
ip bgp policy route-map  
ip bgp policy route-map action  
ip bgp policy route-map aspath-list  
ip bgp policy route-map asprepend  
ip bgp policy route-map community  
ip bgp policy route-map community-list  
ip bgp policy route-map community-mode  
ip bgp policy route-map lpref  
ip bgp policy route-map lpref-mode  
ip bgp policy route-map match-community  
ip bgp policy route-map match-mask  
ip bgp policy route-map match-prefix  
ip bgp policy route-map match-prefix6  
ip bgp policy route-map match-regexp  
ip bgp policy route-map med  
ip bgp policy route-map med-mode  
ip bgp policy route-map origin  
ip bgp policy route-map prefix-list  
ip bgp policy route-map prefix6-list  
ip bgp policy route-map weight  
ip bgp policy route-map community-strip  
show ip bgp policy aspath-list  
show ip bgp policy community-list  
show ip bgp policy prefix-list  
show ip bgp policy prefix6-list  
show ip bgp policy route-map  
| BGP Graceful Restart Commands | ip bgp graceful-restart  
ip bgp graceful-restart restart-interval  
| IPv6 Global BGP Commands | ipv6 bgp unicast  
show ipv6 bgp path  
show ipv6 bgp routes  
| IPv6 BGP Network Configuration Commands | ipv6 bgp network  
ipv6 bgp network community  
ipv6 bgp network local-preference  
ipv6 bgp network metric  
ipv6 bgp network admin-state  
show ipv6 bgp network  |
### IPv6 BGP Neighbor (Peer) Configuration Commands

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 bgp neighbor</td>
</tr>
<tr>
<td>ipv6 bgp neighbor ttl-security</td>
</tr>
<tr>
<td>ipv6 bgp neighbor activate-ipv4</td>
</tr>
<tr>
<td>ipv6 bgp neighbor activate-ipv6</td>
</tr>
<tr>
<td>ipv6 bgp neighbor ipv6-nexthop</td>
</tr>
<tr>
<td>ipv6 bgp neighbor admin-state</td>
</tr>
<tr>
<td>ipv6 bgp neighbor clear</td>
</tr>
<tr>
<td>ipv6 bgp neighbor auto-restart</td>
</tr>
<tr>
<td>ipv6 bgp neighbor remote-as</td>
</tr>
<tr>
<td>ipv6 bgp neighbor timers</td>
</tr>
<tr>
<td>ipv6 bgp neighbor maximum-prefix</td>
</tr>
<tr>
<td>ipv6 bgp neighbor next-hop-self</td>
</tr>
<tr>
<td>ipv6 bgp neighbor conn-retry-interval</td>
</tr>
<tr>
<td>ipv6 bgp neighbor default-originate</td>
</tr>
<tr>
<td>ipv6 bgp neighbor update-source</td>
</tr>
<tr>
<td>ipv6 bgp neighbor ipv4-nexthop</td>
</tr>
<tr>
<td>ipv6 bgp neighbor advertisement-interval</td>
</tr>
<tr>
<td>ipv6 bgp neighbor description</td>
</tr>
<tr>
<td>ipv6 bgp neighbor ebgp-multihop</td>
</tr>
<tr>
<td>ipv6 bgp neighbor update-source-address</td>
</tr>
<tr>
<td>ipv6 bgp neighbor passive</td>
</tr>
<tr>
<td>ipv6 bgp neighbor remove-private-as</td>
</tr>
<tr>
<td>ipv6 bgp neighbor soft-reconfiguration</td>
</tr>
<tr>
<td>ipv6 bgp neighbor stats-clear</td>
</tr>
<tr>
<td>ip bgp confederation neighbor6</td>
</tr>
<tr>
<td>ipv6 bgp neighbor in-aspathlist</td>
</tr>
<tr>
<td>ipv6 bgp neighbor in-communitylist</td>
</tr>
<tr>
<td>ipv6 bgp neighbor in-prefixlist</td>
</tr>
<tr>
<td>ipv6 bgp neighbor in-prefix6list</td>
</tr>
<tr>
<td>ipv6 bgp neighbor out-aspathlist</td>
</tr>
<tr>
<td>ipv6 bgp neighbor out-communitylist</td>
</tr>
<tr>
<td>ipv6 bgp neighbor out-prefixlist</td>
</tr>
<tr>
<td>ipv6 bgp neighbor out-prefix6list</td>
</tr>
<tr>
<td>ipv6 bgp neighbor route-map</td>
</tr>
<tr>
<td>ipv6 bgp neighbor clear soft</td>
</tr>
<tr>
<td>ipv6 bgp neighbor route-reflector-client</td>
</tr>
<tr>
<td>ipv6 bgp neighbor md5 key</td>
</tr>
<tr>
<td>bgp neighbor check-first-as</td>
</tr>
<tr>
<td>show ipv6 bgp neighbors</td>
</tr>
<tr>
<td>show ipv6 bgp neighbors statistics</td>
</tr>
<tr>
<td>show ipv6 bgp neighbors policy</td>
</tr>
<tr>
<td>show ipv6 bgp neighbors timers</td>
</tr>
</tbody>
</table>
ip load bgp

Loads the BGP protocol software into running memory on the router. The image file containing BGP should already be resident in flash memory before issuing this command.

ip load bgp

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• This command requires that the BGP software be resident in flash memory in the active directory.

• Enter this command in the router’s configuration file (boot.cfg) to ensure BGP software is running after a reboot.

• The command does not administratively enable BGP on the router; BGP will be disabled after issuing this command. You must issue the ip bgp admin-state to start the BGP protocol.

Examples

-> ip load bgp

Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp autonomous-system**: Configures the Autonomous system number for this BGP router.
- **ip bgp admin-state**: Administratively enables or disables BGP.

MIB Objects

- **alaVrConfigTable**
  - **alaVrConfigBgpStatus**
**ip bgp admin-state**

Administratively enables or disables BGP. The BGP protocol will not be active until you enable it using this command.

`ip bgp admin-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BGP.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BGP.</td>
</tr>
</tbody>
</table>

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- You must first load the BGP software into running memory using the `ip load bgp` command before initiating this command.
- Many BGP commands require that the protocol be disabled (`ip bgp admin-state`) before issuing them.

---

**Examples**

```
-> ip bgp admin-state enable
-> ip bgp admin-state disable
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `ip load bgp` Loads the BGP software.

---

**MIB Objects**

- `alaBgpGlobal`
ip bgp autonomous-system

Configures the Autonomous System (AS) number for this router. This number identifies this BGP speaker (this router) instance to other BGP routers. The AS number for a BGP speaker determines whether it is an internal or an external peer in relation to other BGP speakers. BGP routers in the same AS are internal peers while BGP routers in different ASs are external peers. BGP routers in the same AS exchange different routing information with each other than they exchange with BGP routers in external ASs. BGP speakers append their AS number to routes passing through them; this sequence of AS numbers is known as a route’s AS path.

Syntax Definitions

value The AS number in the asplain, asdot+, or asdot formats.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- A router can belong to only one AS. Do not specify more than one AS value for each router.
- The BGP protocol must be disabled (using the ip bgp admin-state command) before using this command.
- The 4-octet ASN is represented in one of three ways:
  - asplain (simple decimal notation)
  - asdot+ (two 16-bit values as low-order and high-order)
  - asdot (a mixture of asplain and asdot+).

Examples

- `ip bgp autonomous-system 64724`

The following examples show how to configure the local BGP ASN as 65535 in the three different formats:
- `ip bgp autonomous-system 65535` (asplain format)
-> ip bgp autonomous-system 0.65535 (asdot+ format)
-> ip bgp autonomous-system 65535 (asdot format)
The following examples show how to configure the local BGP ASN as 65538 in the three different formats:
-> ip bgp autonomous-system 65538 (asplain format)
-> ip bgp autonomous-system 1.2 (asdot+ format)
-> ip bgp autonomous-system 1.2 (asdot format)

Release History
Release 7.1.1; command was introduced.
Release 7.3.3; support for 4-octet ASN was added.

Related Commands
ip bgp admin-state Enables and disables the BGP protocol.
ip bgp neighbor remote-as Assigns an AS number to this BGP peer.

MIB Objects
alaBgpGlobal
alaBgpAutonomousSystemNumber
ip bgp bestpath as-path ignore

Indicates whether AS path comparison will be used in route selection. The AS path is the sequence of ASs through which a route has traveled. A shorter AS path is preferred over a longer AS path. The AS path is always advertised in BGP route updates. This command informs BGP to use the length of the AS path as a criteria for determining the best route.

ip bgp bestpath as-path ignore
no ip bgp bestpath as-path ignore

Syntax Definitions

N/A

Defaults

This command is enabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable this feature after it has been enabled.
- AS path comparison does not consider the type of links connecting the ASs along the path. In some cases a longer path over very fast connections may be a better route than a shorter path over slower connections. For this reason the AS path should not be the only criteria used for route selection. BGP considers local preference before AS path when making path selections.
- The BGP protocol must be disabled (using the ip bgp admin-state command) before using this command.

Examples

- -> ip bgp bestpath as-path ignore
- -> no ip bgp bestpath as-path ignore

Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp aggregate-address as-set**: Specifies whether AS path aggregation is to be performed or not.
- **ip bgp policy aspath-list**: Creates or removes an AS path list.
- **ip bgp default local-preference**: Configures the default local preference (lpref) value to be used when advertising routes.

MIB Objects

- **alaBgpGlobal**
  - **alaBgpAsPathCompare**
**ip bgp cluster-id**

Configures a BGP cluster ID when there are multiple, redundant, route reflectors in a cluster. This command is not necessary for configurations containing only one route reflector.

**ip bgp cluster-id ip_address**

---

**Syntax Definitions**

- **ip_address**: 32-bit IP address that is the Cluster ID of the router acting as a route reflector.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- In a route-reflection configuration where there are multiple route-reflectors in a cluster, use this command to configure this cluster ID. Configuring multiple route-reflectors enhances redundancy and avoids a single point of failure. When there is only one reflector in a cluster, the router ID of the reflector is used as the cluster-ID.

- The BGP protocol must be disabled (using the `ip bgp admin-state` command) before using this command.

- Using many redundant reflectors in a single cluster places demands on the memory required to store routes for all redundant reflectors’ peers.

**Examples**

```
-> ip bgp cluster-id 1.2.3.4
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `ip bgp admin-state` Enables and disables BGP.
- `ip bgp client-to-client reflection` Enables route reflection and sets this speaker as the route reflector.

MIB Objects

- `alaBgpGlobal`
- `alaBgpClusterId`
**ip bgp default local-preference**

Configures the default local preference (lpref) value to be used when advertising routes. A higher local preference value is preferred over a lower value. The local preference value is sent to all BGP peers in the local autonomous system; it is not advertised to external peers.

**Syntax Definitions**

```plaintext
value
```

The default local preference value for this router. The valid range is 0–4294967295.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>100</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to restore the default value.
- Unless a route is specifically configured for a different local preference value it will default to value you specify in this command. This value is used for routes learned from external autonomous systems (the local preference value is not advertised in routes received from external peers) and for aggregates and networks that do not already contain local preference values.
- This value is specific to the router so it can compare its own local preference to those received in advertised paths. If other routers belong to the same AS, then they should use the same default local preference value.
- The BGP protocol must be disabled (using the `ip bgp admin-state` command) before using this command.

**Examples**

```plaintext
-> ip bgp default local-preference 200
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp aggregate-address local-preference** Sets the local preference for a BGP aggregate.
- **ip bgp network local-preference** Sets the local preference for a BGP network.

MIB Objects

- **alaBgpGlobal**
  - **alaBgpDefaultLocalPref**
ip bgp fast-external-failover

Enables fast external failover (FEFO). When enabled, FEFO resets a session when a link to a directly connected external peer is operationally down. The BGP speaker will fall back to Idle and then wait for a connection retry by the external peer that went down.

- **ip bgp fast-external-failover**
- **no ip bgp fast-external-failover**

**Syntax Definitions**

N/A

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to disable Fast External Failover.
- When enabled, this command allows BGP to take immediate action when a directly connected interface, on which an external BGP session is established, goes down. Normally BGP relies on TCP to manage peer connections. Fast External failover improves upon TCP by resetting connections as soon as they go down.
- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

**Examples**

- `-> ip bgp fast-external-failover`
- `-> no ip bgp fast-external-failover`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ip bgp neighbor clear**  
  Restarts a BGP peer.

- **ip bgp neighbor auto-restart**  
  Enables or disables BGP peer automatic restart.

- **ip bgp neighbor timers**  
  Configures the time interval between KEEPALIVE messages sent by this peer and the tolerated hold time interval, in seconds, for messages to this peer from other peers.

**MIB Objects**

- `alaBgpFastExternalFailOver`
**ip bgp always-compare-med**

Enables or disables Multi-Exit Discriminator (MED) comparison between peers in different autonomous systems. The MED value is considered when selecting the best path among alternatives; it indicates the weight for a particular exit point from the AS. A path with a lower MED value is preferred over a path with a higher MED value.

**ip bgp always-compare-med**

**no ip bgp always-compare-med**

---

### Syntax Definitions

N/A

### Defaults

This command is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to disable MED comparison for external peers.

- By default, BGP only compares MEDs from the same autonomous system when selecting routes. Enabling this command forces BGP to also compare MEDs values received from external peers, or other autonomous systems.

- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

### Examples

```
-> ip bgp always-compare-med
-> no ip bgp always-compare-med
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

`ip bgp bestpath med missing-as-worst`  Configures the MED parameter when it is missing in a BGP path.

**MIB Objects**

`alaBgpGlobal`  `alaBgpMedAlways`
ip bgp bestpath med missing-as-worst

Configures the MED parameter when it is missing in a BGP path.

ip bgp bestpath med missing-as-worst
no ip bgp bestpath med missing-as-worst

Syntax Definitions

N/A

Defaults

By default this command is disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

| Platform  | 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900V72/C32 | 6900X48C6/T48C6 | X48C4E/V48C8 | C32E/T24C2 | X24C2 | 9900 |
|-----------|------|------|------|-------|------|-------|------|------|-------------|---------------|-------------|---------|-------|------|------|
| Supported | No   | No   | No   | No    | Yes  | Yes   | Yes  | Yes  | Yes         | Yes           | Yes         | Yes      | Yes   | Yes   |

Usage Guidelines

- Use the **no** form of this command to disable missing MEDs as worst.

- This command is used to specify how a missing MED in an external BGP path is to be treated for route selection purposes. The default behavior is to treat missing MEDs as zero (best). This command allows you to treat missing MEDs as worst (2^{32}-1) for compatibility reasons.

- The BGP protocol must be disabled (using the **ip bgp admin-state** command) before using this command.

Examples

-> ip bgp bestpath med missing-as-worst
-> no ip bgp bestpath med missing-as-worst

Release History

Release 7.1.1; command was introduced.

Related Commands

- **ip bgp always-compare-med** Forces BGP to consider MED values from external routes.

MIB Objects

- alaBgpGlobal
ip bgp bestpath med missing-as-worst
ip bgp client-to-client reflection

Enables or disables this BGP speaker (router) to be a route reflector. Route reflectors advertise routing information to internal BGP peers, referred to as clients. BGP requires all internal routers to know all routes in an AS. This requirement demands a fully meshed (each router has a direct connection to all other routers in the AS) topology. Route reflection loosens the fully meshed restriction by assigning certain BGP routers as route reflectors, which take on the responsibility of advertising routing information to local BGP peers.

ip bgp client-to-client reflection

no ip bgp client-to-client reflection

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable the speaker as a route reflector.

- In addition to defining this router as the route reflector, this command also enable route reflection for this cluster. After setting this command this reflector will begin using route reflection behavior when communicating to client and non-client peers.

- Once route reflectors are configured, you need to indicate the clients (those routers receiving routing updates from the reflectors) for each route reflector. Use the ip bgp neighbor route-reflector-client command to configure clients.

- The BGP protocol must be disabled (using the ip bgp admin-state command) before using this command.

Examples

- -> ip bgp client-to-client reflection
- -> no ip bgp client-to-client reflection
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bgp admin-state**  
  Administratively disables BGP in this router.

- **ip bgp neighbor route-reflector-client**  
  Configures a BGP peer to be a client to the this route reflector.

**MIB Objects**

- **alaBgpGlobal**
  - **alaBgpRouteReflection**
ip bgp as-origin-interval

Specifies the frequency at which routes local to the autonomous system are advertised. These advertisements are also referred to as UPDATE messages. This interval applies to advertisements to internal peers.

ip bgp as-origin-interval seconds

no ip bgp as-origin-interval

Syntax Definitions

seconds The update interval in seconds. The valid range is 1–65535.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>15</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to reset the feature to the default value.
- A lower value may increase the likelihood of route flapping as route status is updated more frequently.

Examples

-> ip bgp as-origin-interval 15

-> no ip bgp as-origin-interval

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp neighbor advertisement-interval Set the route advertisement interval for external peers.

MIB Objects

alaBgpGlobal
ip bgp as-origin-interval

alaBgpAsOriginInterval
**ip bgp synchronization**

Enables or disables synchronization of BGP prefixes with AS-internal routing information. Enabling this command will force the BGP speaker to advertise prefixes only if the prefixes are reachable through AS-internal routing protocols (IGPs like RIP and OSPF).

```
ip bgp synchronization
no ip bgp synchronization
```

**Syntax Definitions**

N/A

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable IGP synchronization.

- A BGP router is not supposed to advertise routes learned through internal BGP updates unless those routes are also known by the primary internal routing protocol (e.g., RIP or OSPF). However, requiring all routers in an AS to know all external routes places a heavy burden on routers focusing mainly on Intra-AS routing. Therefore, disabling synchronization avoids this extra burden on internal routers. As long as all BGP routers in an AS are fully meshed (each has a direct connection to all other BGP routers in the AS) then the problem of unknown external router should not be a problem and synchronization can be disabled.

- By default, synchronization is disabled and the BGP speaker can advertise a route without waiting for the IGP to learn it. When the autonomous system is providing transit service, BGP should not propagate IGP paths until the IGP prefixes themselves are known to be reachable through IGP. If BGP advertises such routes before the IGP routers have learned the path, they will drop the packets causing a blackhole.

- The BGP protocol must be disabled (using the `ip bgp admin-state` command) before using this command.

**Examples**

```
-> ip bgp synchronization
```
-> no ip bgp synchronization

**Release History**
Release 7.1.1; command was introduced.

**Related Commands**
show ip bgp
Displays the current global settings for the local BGP speaker.

**MIB Objects**
alaBgpGlobal
  alaBgpIgpSynchStatus
**ip bgp confederation identifier**

Sets a confederation identification value for the local BGP speaker (this router). A confederation is a grouping of sub-ASs into a single AS. To peers outside a confederation, the confederation appears to be a single AS. Within the confederation multiple ASs may exist and even exchange information with each other as using external BGP (EBGP).

`ip bgp confederation identifier value`

---

**Syntax Definitions**

`value` The confederation identification value. The valid range is 0–65535.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to restore the default value.
- A value of 0 means this local speaker is not a member of any confederation.
- The BGP protocol must be disabled (using the `ip bgp admin-state` command) before using this command.
- Use this command in conjunction with the `ip bgp confederation neighbor` command to specify those peers that are a members of the same confederation as the local BGP speaker.

---

**Examples**

`-> ip bgp confederation identifier 3`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `ip bgp autonomous-system` Sets the AS number for this router.
- `ip bgp confederation neighbor` Specifies peers that are members of a confederation.

MIB Objects

- `alaBgpGlobal`
- `alaBgpConfId`
ip bgp maximum-paths

Enables or disables support for multiple equal paths. When multipath support is enabled and the path selection process determines that multiple paths are equal when the router-id is disregarded, then all equal paths are installed in the hardware forwarding table. When multipath support is disabled, only the best route entry is installed in the hardware forwarding table.

ip bgp maximum-paths

no ip bgp maximum-paths

Syntax Definitions

N/A

Defaults

This command is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable support for multiple equal cost paths.
- The BGP protocol must be disabled (using the ip bgp admin-state command) before using this command.

Examples

- ip bgp maximum-paths
- no ip bgp maximum-paths

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip bgp

Displays the current global settings for the local BGP speaker.

MIB Objects

alaBgpGlobal
BGP Commands

ip bgp maximum-paths

alaBgpMultiPath
**ip bgp log-neighbor-changes**

Enables or disables the logging of peer state changes. If enabled, this logging tracks changes in the state of BGP peers from ESTABLISHED to IDLE and from IDLE to ESTABLISHED. Viewing peer state logging requires that certain debug parameters be set.

```
ip bgp log-neighbor-changes
no ip bgp log-neighbor-changes
```

---

**Syntax Definitions**

N/A

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BGP protocol must be disabled (using the `ip bgp admin-state` command) before using this command.

**Examples**

```
-> ip bgp log-neighbor-changes
-> no ip bgp log-neighbor-changes
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp admin-state` Disables BGP within the router.

**MIB Objects**

- `alaBgpGlobal`
- `alaBgpPeerChanges`
**ip bgp dampening**

Enables or disables BGP route dampening or the suppression of unstable routes. Route dampening helps to control the advertisement of routes that are going up and then down at an abnormally high rate. Routes that are changing states (available then unavailable) are said to be **flapping**.

```
ip bgp dampening [half-life half_life reuse reuse suppress suppress max-suppress-time max_suppress_time]
no ip bgp dampening
```

**Syntax Definitions**

- **half_life**
  The half-life duration, in seconds. The valid range is 0–65535.
- **reuse**
  The number of route withdrawals set for the re-use value. The valid range is 1–9999.
- **suppress**
  The dampening cutoff value. The valid range is 1–9999.
- **max_suppress_time**
  The maximum number of seconds a route can be suppressed. The valid range is 0–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>half_life</td>
<td>300</td>
</tr>
<tr>
<td>reuse</td>
<td>200</td>
</tr>
<tr>
<td>suppress</td>
<td>300</td>
</tr>
<tr>
<td>max_suppress_time</td>
<td>1800</td>
</tr>
</tbody>
</table>

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable dampening.
- BGP dampening is disabled by default. When enabled, route dampening suppresses routes that are unstable, or “flapping,” and disrupting the network.
- BGP dampening of IPv6 route flaps is currently not supported.
This command enables dampening and can also be used to change the default times for the dampening variables.

Use the dampening variables to set penalties, suppression limits, and reuse values for flapping routes.

The half-life value configures the half-life duration for a reachable route. After the time interval specified in this command, the penalty value for the route will be reduced by half. This command sets the duration in seconds during which the accumulated stability value is reduced by half if the route is considered reachable, whether suppressed or not. A larger value may be desirable for routes that are known for their instability. A larger value will also result in a longer suppression time if the route exceeds the flapping rate.

The reuse value configures the number of route withdrawals necessary to begin readvertising a previously suppressed route. If the penalty value for a suppressed route fall below this value, then it will be advertised again. This command sets the reuse value, expressed as a number of route withdrawals. When the stability value for a route reaches or falls below this value, a previously suppressed route will be advertised again. The instability metric for a route is decreased by becoming more stable and by passing half-life time intervals.

The suppress value configures the cutoff value, or number of route withdrawals, at which a flapping route is suppressed and no longer advertised to BGP peers. This value is expressed as a number of route withdrawals. When the stability value for a route exceeds this cutoff value, the route advertisement is suppressed.

The max-suppress-time value configures the maximum time (in seconds) a route can be suppressed. This time is also known as the maximum holdtime or the maximum instability value. Once this time is reached the route flap history for a route will be deleted and the route will be advertised again (assuming it is still reachable). This maximum holdtime as applied on an individual route basis. Each suppressed route will be held for the amount of time specified in this command unless the route is re-advertised by falling below the reuse value.

Entering the command with no variables returns the variables back to their defaults.

Examples

```
-> ip bgp dampening
-> ip bgp dampening half-life 20 reuse 800 suppress 60 max-suppress-time 40
-> no ip bgp dampening
```

Release History

Release 7.1.1; command was introduced.

Related Commands

- **ip bgp dampening clear**: Clears the dampening history data for all routes on the router, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.
- **show ip bgp dampening**: Displays the BGP route dampening settings.
- **show ip bgp dampening-stats**: Displays BGP dampening statistics.
**MIB Objects**

`alaBgpGlobal`
- `alaBgpDampening`
- `alaBgpDampMaxFlapHistory`
- `alaBgpDampHalfLifeReach`
- `alaBgpDampReuse`
- `alaBgpDampCutOff`
ip bgp dampening clear

Clears the dampening history data for all routes on the router, resetting route flap counters and unsuppressing any routes that had been suppressed due to route flapping violations.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to clear all of the currently stored information on routes for dampening purposes. When this command is entered, all route information in regards to dampening is cleared.
- BGP dampening of IPv6 route flaps is currently not supported.

**Examples**

```
-> ip bgp dampening clear
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp dampening`: Enables or disables route dampening.

**MIB Objects**

- `alaBgpGlobal`
- `alaBgpDampeningClear`
**ip bgp asn-format**

Configures the display format to be used when displaying 4-octet ASNs.

*ip bgp asn-format {asdot | asplain}*

**Syntax Definitions**

- **asdot**: A mixture of asplain and asdot+.
- **asplain**: Simple decimal notation.

**Defaults**

The default is **asplain**.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command configures the display format to be used when displaying 4-octet ASNs. This configuration changes only the output format. The input format can be in any mode.

**Examples**

- `-> ip bgp asn-format asdot`

**Release History**

Release 7.3.3; command was introduced.

**Related Commands**

- **ip bgp autonomous-system**: Configures the Autonomous System (AS) number for this router.
- **show ip bgp**: Displays the current global settings for the local BGP speaker.

**MIB Objects**

- **alaBgpGlobal**
- **alaBgpAsnFormat**
**ip bgp aggregate-address**

Creates and deletes a BGP aggregate route. Aggregate routes are used to reduce the size of routing tables by combining the attributes of several different routes and allowing a single aggregate route to be advertised to peers.

The base command (**ip bgp aggregate-address**) may be used with other keywords to set up aggregate address configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

Note that only one of the following optional keywords is specified with each use of the base command. Keywords are not combined together in a single command.

```plaintext
ip bgp aggregate-address ip_address ip_mask
   [admin-state {enable | disable}]
   [as-set]
   [community string]
   [local-preference value]
   [metric metric]
   [summary-only]

no ip bgp aggregate-address ip_address ip_mask
```

**Syntax Definitions**

- **ip_address** 32-bit IP address to be used as the aggregate address.
- **ip_mask** 32-bit subnet mask that determines how many bits of the IP address denote the network number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete an aggregate route.
- This command allows administrative operations on a BGP aggregate. You must still enable the aggregate route through the **ip bgp aggregate-address admin-state** command.
You cannot aggregate an address (for example, 100.10.0.0) if you do not have at least one more-specific route of the address (for example, 100.10.20.0) in the BGP routing table.

Only the aggregate is advertised unless aggregate summarization is disabled using the `ip bgp aggregate-address summary-only` command.

**Examples**

```bash
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0
-> no ip bgp aggregate-address 172.22.2.0 255.255.255.0
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp aggregate-address summary-only`: Enables or disables aggregate summarization, which suppresses more-specific routes.

**MIB Objects**

- `alaBgpAggrAddr`
- `alaBgpAggrSet`
- `alaBgpAggrCommunity`
- `alaBgpAggrLocalPref`
- `alaBgpAggrMetric`
- `alaBgpAggrSummarize`
- `alaBgpAggrMask`
ip bgp aggregate-address admin-state

Enables or disables a BGP aggregate route.

`ip bgp aggregate-address ip_address ip_mask admin-state {enable | disable}`

**Syntax Definitions**

- `ip_address`: 32-bit IP address for this aggregate route.
- `ip_mask`: 32-bit subnet mask that determines how many bits of the network address denote the network number.
- `enable`: Enables this aggregate route.
- `disable`: Disables this aggregate route.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Configure all aggregate route parameters before enabling the aggregate with this command. Use the `ip bgp asn-format` command to configure individual aggregate parameters.
- The `show ip bgp path` command displays every aggregate currently defined.

**Examples**

```
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 admin-state enable
-> ip bgp aggregate-address 172.22.2.0 255.255.255.0 admin-state disable
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp asn-format**
  - Creates an aggregate route.
- **show ip bgp path**
  - Displays aggregate routes.

MIB Objects

- **alaBgpAggrTable**
  - **alaBgpAggrAddr**
  - **alaBgpAggrMask**
ip bgp aggregate-address as-set

Specifies whether AS path aggregation is to be performed or not. AS path aggregation takes the AS path for all routes in this aggregate and creates a new AS path for the entire aggregate. This aggregated AS path includes all the ASs from the routes in the aggregate, but it does not repeat AS numbers if some routes in the aggregate include the same AS in their path.

Syntax:

*ip bgp aggregate-address ip_address ip_mask as-set*

*no ip bgp aggregate-address ip_address ip_mask as-set*

**Syntax Definitions**

*ip_address* 32-bit IP address.

*ip_mask* 32-bit subnet mask that determines how many bits of the IP address denote the network number.

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to disable the *as-set* option.
- When AS path aggregation is disabled (the default), the AS path for the aggregate defaults to the AS number of the local BGP speaker (configured in the *ip bgp autonomous-system* command).
- If AS path aggregation is enabled, a flap in a more specific path’s AS path will cause a flap in the aggregate as well.
- Do not use this command when aggregating many paths because of the numerous withdrawals and updates that must occur as path reachability information for the summarized routes changes.

**Examples**

- `-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set`
- `-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 as-set`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ip bgp asn-format**

Creates and deletes a BGP aggregate route.

MIB Objects

alaBgpAggrTable

- alaBgpAggrAddr
- alaBgpAggrMask
- alaBgpAggrSet
**ip bgp aggregate-address community**

Defines a community for an aggregate route created by the `ip bgp aggregate-address` command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS number.

`ip bgp aggregate-address ip_address ip_mask community {none | no-export | no-advertise | no-export-subconfed | num:num}`

**Syntax Definitions**

- `ip_address`: 32-bit IP address of the aggregate route.
- `ip_mask`: 32-bit subnet mask that determines how many bits of the IP address denote the network number.
- `none`: Removes the community restrictions on the community section of the route map.
- `no-export`: Routes in this community are advertised within the AS but not beyond the local AS.
- `no-advertise`: Routes in this community are not advertised to any peer.
- `no-export-subconfed`: Routes in this community are not advertised to any external BGP peer.
- `num:num`: The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>no-export</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The value of AS:NN is `num:num:num` if using asdot or asdot+ notation and is `num:num` if using asplain format.
- To revert the aggregate community string to the default value, set the community string to `none`. 
**Examples**

-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community no-export
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 community none

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to `community` string.

**Related Commands**

*ip bgp asn-format* Creates and deletes a BGP aggregate route.

**MIB Objects**

alaBgpAggrTable
  alaBgpAggrAddr
  alaBgpAggrMask
  alaBgpAggrCommunity
ip bgp aggregate-address local-preference

Configures the local preference attribute value for this BGP aggregate. This value will override the default local preference value; it is used when announcing this aggregate to internal peers.

ip bgp aggregate-address ip_address ip_mask local-preference value
no ip bgp aggregate-address ip_address ip_mask local-preference value

Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>An IP address for the aggregate route.</td>
</tr>
<tr>
<td>ip_mask</td>
<td>32-bit subnet mask that determines how many bits of the IP address denote the network number.</td>
</tr>
<tr>
<td>value</td>
<td>The local preference attribute. The valid range is 0–4294967295.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to set the local preference back to the default value.
- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the ip bgp default local-preference command).

Examples

- `-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200`
- `-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 local-preference 200`

Release History

Release 7.1.1; command was introduced.
Related Commands

**ip bgp default local-preference**  Sets the default local preference value for this AS.

MIB Objects

alaBgpAggrTable
  alaBgpAggrAddr
  alaBgpAggrMask
  alaBgpAggrLocalPref
ip bgp aggregate-address metric

Configures the MED attribute value for a BGP aggregate. This value is used when announcing this aggregate to internal peers; it indicates the best exit point from the AS.

```
ip bgp aggregate-address ip_address ip_mask metric value
no ip bgp aggregate-address ip_address ip_mask metric value
```

Syntax Definitions

- **ip_address**: A 32-bit IP address.
- **ip_mask**: 32-bit subnet mask that determines how many bits of the IP address denote the network number.
- **value**: The MED attribute. The valid range is 0–4294967295.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to reset the aggregate metric back to its default value.
- The default value of zero indicates that a MED will not be sent for this aggregate. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the **ip bgp bestpath med missing-as-worst** command.

Examples

```
-> ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
-> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 metric 0
```

Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp bestpath med missing-as-worst**
  Configures the MED for paths that do not contain a MED value.

- **ip bgp always-compare-med**
  Forces BGP to use the MED for comparison of external routes.

MIB Objects

- **alaBgpAggrTable**
  alaBgpAggrAddr
  alaBgpAggrMask
  alaBgpAggrMetric
ip bgp aggregate-address summary-only

Enables or disables aggregate summarization, which suppresses more-specific routes. Disabling aggregate summarization means that more-specific routes will be announced to BGP peers (internal and external peers).

ip bgp aggregate-address ip_address ip_mask summary-only

no ip bgp aggregate-address ip_address ip_mask summary-only

Syntax Definitions

- ip_address: IP address for the aggregate route.
- ip_mask: 32-bit subnet mask that determines how many bits of the IP address denote the network number.

Defaults

This command is enabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable this feature.
- This command specifies whether more-specific routes should be announced or suppressed.
- By default, aggregate summarization is enabled, which means that only the aggregate entry (for example, 100.10.0.0) is advertised. Advertisements of more-specific routes (for example, 100.10.20.0) are suppressed.

Examples

- -> ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only
- -> no ip bgp aggregate-address 172.22.2.115 255.255.255.0 summary-only

Release History

Release 7.1.1; command was introduced.
Related Commands

**ip bgp asn-format**

Creates and deletes a BGP aggregate route.

MIB Objects

alaBgpAggrTable
  - alaBgpAggrAddr
  - alaBgpAggrMask
  - alaBgpAggrSummarize
ip bgp network

Creates or deletes a BGP network. A network must be known to the local BGP speaker; it also must originate from the local BGP speaker. The network may be directly connected, dynamically learned, or static.

In lieu of these options, the base command (ip bgp network) may be used with other keywords to set up network configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a no form to remove the parameter or return it to its default.

```
ip bgp network ip_address ip_mask
    [community string]
    [local-preference value]
    [metric metric]
    [admin-state {enable | disable}]
```

```
no ip bgp network ip_address ip_mask
```

### Syntax Definitions

- **ip_address**: 32-bit IP address.
- **ip_mask**: 32-bit subnet mask that determines how many bits of the IP address denote the network number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to delete a local network.
- Creating and enabling a network entry indicates to BGP that this network should originate from this router. The network specified must be known to the router, whether it is connected, static, or dynamically learned.
- You can create up to 200 network entries. The basic `show ip bgp path` command will display every network currently defined.
- This command allows administrative operations on a BGP network. You must still enable the network through the `ip bgp network admin-state` command.
Examples

-> ip bgp network 172.22.2.115 255.255.255.0
-> no ip bgp network 172.22.2.115 255.255.255.0

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp network admin-state    Enables a BGP network.

MIB Objects

alaBgpNetworkTable
  alaBgpNetworkAddr
  alaBgpNetworkMetric
  alaBgpNetworkLocalPref
  alaBgpNetworkCommunity
  alaBgpNetworkMask
ip bgp network admin-state

Enables or disables a BGP network.

```
ip bgp network ip_address ip_mask admin-state {enable | disable}
```

### Syntax Definitions

- **ip_address**: 32-bit IP address.
- **ip_mask**: 32-bit subnet mask that determines how many bits of the IP address denote the network number.
- **enable**: Enables this network.
- **disable**: Disables this network.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Configure all network parameters before enabling this BGP network with this command. Use the **ip bgp network** command to configure individual aggregate parameters.

- You can create up 200 network entries. The **show ip bgp path** command displays every network currently defined.

### Examples

```
-> ip bgp network 172.22.2.115 255.255.255.0 admin-state enable
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **ip bgp network**  
  Create a BGP network.
- **show ip bgp path**  
  Display currently defined BGP networks.

**MIB Objects**

- `alaBgpNetworkTable`
- `alaBgpNetworkAddr`
- `alaBgpNetworkMask`
**ip bgp network community**

Defines a community for a route created by the `ip bgp network` command. Communities are a way of grouping BGP peers that do not share an IP subnet or an AS.

**ip bgp network ip_address ip_mask community {none | no-export | no-advertise | no-export-subconfed | num:num}**

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_address</code></td>
<td>32-bit IP address of the network.</td>
</tr>
<tr>
<td><code>ip_mask</code></td>
<td>32-bit subnet mask that determines how many bits of the IP address denote the network number.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Removes the community restrictions on the community section of the route map.</td>
</tr>
<tr>
<td><code>no-export</code></td>
<td>Routes in this community are advertised within the AS but not beyond the local AS.</td>
</tr>
<tr>
<td><code>no-advertise</code></td>
<td>Routes in this community are not advertised to any peer.</td>
</tr>
<tr>
<td><code>no-export-subconfed</code></td>
<td>Routes in this community are not advertised to any external BGP peer.</td>
</tr>
<tr>
<td><code>num:num</code></td>
<td>The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>none</code></td>
<td><code>none</code></td>
</tr>
<tr>
<td><code>no-export</code></td>
<td><code>none</code></td>
</tr>
<tr>
<td><code>no-advertise</code></td>
<td><code>none</code></td>
</tr>
<tr>
<td><code>no-export-subconfed</code></td>
<td><code>none</code></td>
</tr>
<tr>
<td><code>num:num</code></td>
<td><code>none</code></td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The value of AS:NN is `num.num:num` if using asdot or asdot+ notation and is `num:num` if using asplain format.
- To revert the network community string to the default value, set the community string to `none`. 


**Examples**

-> ip bgp network 172.22.2.115 255.255.255.0 community export
-> ip bgp network 172.22.2.115 255.255.255.0 community none

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to **community** string.

**Related Commands**

ip bgp network  
Creates or deletes a BGP network

**MIB Objects**

alaBgpNetworkTable  
alaBgpNetworkAddr  
alaBgpNetworkMask  
alaBgpNetworkCommunity
ip bgp network local-preference

Defines the local preference value for a route generated by the ip bgp network command. This value will override the default local preference value; it is used when announcing this network to internal peers.

**ip bgp network ip_address ip_mask local-preference value**

**no ip bgp network ip_address ip_mask local-preference value**

**Syntax Definitions**

- **ip_address**: 32-bit IP address.
- **ip_mask**: 32-bit subnet mask that determines how many bits of the IP address denote the network number.
- **value**: The local preference attribute value. The valid range is 0–4294967295.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to return the local preference of the specified network to its default setting.

- You can specify that this route use the default local preference value for the AS by specifying zero (0). In this case the local preference for this route will take the default local preference value set for this AS (defined in the **ip bgp default local-preference** command).

**Examples**

- `-> ip bgp network 172.22.2.115 255.255.255.0 local-preference 600`
- `-> no ip bgp network 172.22.2.115 255.255.255.0 local-preference 600`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp network**  Creates or deletes a BGP network.
- **ip bgp default local-preference**  Sets the default local preference for this AS.

MIB Objects

- alaBgpNetworkTable
  - alaBgpNetworkAddr
  - alaBgpNetworkMask
  - alaBgpNetworkLocalPref
**ip bgp network metric**

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the `ip bgp network` command. This value is used when announcing this network to internal peers; it indicates the best exit point from the AS.

```
ip bgp network ip_address ip_mask metric value
no ip bgp network ip_address ip_mask metric value
```

**Syntax Definitions**

- `ip_address`: 32-bit IP address.
- `ip_mask`: 32-bit subnet mask that determines how many bits of the IP address denote the network number.
- `value`: A MED attribute value. The valid range is 0–4294967295.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to return the metric for this network to its default value.

- The default value of zero indicates that a MED will not be sent for this network. When a MED value is missing for a route, BGP will determine a MED value based upon the settings specified in the `ip bgp bestpath med missing-as-worst` command.

**Examples**

```
-> ip bgp network 172.22.2.115 255.255.255.0 metric 100
-> no ip bgp network 172.22.2.115 255.255.255.0 metric 100
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp network**: Creates or deletes a BGP network.
- **ip bgp bestpath med missing-as-worst**: Specifies the MED value when it is missing.

MIB Objects

- **alaBgpNetworkTable**
  - **alaBgpNetworkAddr**
  - **alaBgpNetworkMask**
  - **alaBgpNetworkMetric**
ip bgp neighbor

Creates or deletes a BGP peer.

**ip bgp neighbor ip_address**

**no ip bgp neighbor ip_address**

---

**Syntax Definitions**

**ip_address**

32-bit IP address of the new BGP peer.

**Defaults**

No peers configured.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete a BGP peer.
- You must still enable a BGP peer after creating it. A BGP peer is enabled using the **ip bgp neighbor admin-state** command.
- Once created, a BGP peer cannot be enabled until it is assigned an autonomous system number using the **ip bgp neighbor remote-as** command.

**Examples**

- `-> ip bgp neighbor 172.22.2.115`
- `-> no ip bgp neighbor 172.22.2.115`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip bgp neighbor admin-state`  
  Enable or disable a BGP peer.
- `ip bgp neighbor remote-as`  
  Configure the AS number for the peer.

**MIB Objects**

- `alaBgpPeerTable`
- `alaBgpPeerAddr`
**ip bgp neighbor ttl-security**

Configures the Generalized TTL Security Mechanism (GTSM) for the BGP peer. GTSM allows to set the maximum number of hops for the IP packets between the switch and the peer. If the maximum number of hops exceeds, the packet is dropped at the NI.

`ip bgp neighbor ip_address ttl-security num`

`ip bgp neighbor ip_address no ttl-security`

**Syntax Definitions**

- `ip_address` : 32-bit IP address of the BGP peer.
- `num` : The maximum number of hops between the switch and the peer. The valid range for GTSM is 0 to 255.

**Defaults**

By default GTSM is disabled for communication with the peer.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- GTSM must be manually enabled on both peers in a connection.
- When GTSM is enabled, eBGP multihop must be disabled or vise-versa.
- Use the `no` form of this command to disable GTSM.

**Examples**

- `-> ip bgp neighbor 172.22.2.115 ttl-security 6`
- `-> ip bgp neighbor 172.22.2.115 no ttl-security`

**Release History**

Release 8.4.1; command was introduced.
Related Commands

show ip bgp neighbors

Displays the configured IPv4 BGP peers.

MIB Objects

alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerTTLSecurityHops
**ip bgp neighbor activate-ipv4**

Enables the advertisement of IPv4 unicast capability to the IPv4 BGP peer.

```
ip bgp neighbor ip_address [activate-ipv4]
no ip bgp neighbor ip_address [activate-ipv4]
```

---

**Syntax Definitions**

- `ip_address` 32-bit IP address of the BGP peer.
- `activate-ipv4` Enable the advertisement of IPv4 unicast capability to the IPv4 BGP peer.

**Defaults**

By default, the command is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to disable the advertisement of IPv4 unicast capability to IPv4 BGP peer.

**Examples**

```
-> ip bgp neighbor 172.22.2.115 activate-ipv4
-> no ip bgp neighbor 172.22.2.115 activate-ipv4
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- **ip bgp neighbor** Creates or deletes a BGP peer.

MIB Objects

- `alaBgpPeerTable`
  - `alaBgpPeerAddr`
  - `alaBgpPeerActivateIpv4`
ip bgp neighbor admin-state

Enables or disables a BGP peer.

```
ip bgp neighbor ip_address admin-state {enable | disable}
```

### Syntax Definitions

- `ip_address` 32-bit IP address of the BGP peer.
- `enable` Enables this peer.
- `disable` Disables this peer.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- You must first create a peer and assign it an IP address using the `ip bgp neighbor` command before enabling the peer.
- Configure all BGP peer related commands before enabling a peer using this command. Once you enable the peer it will begin sending BGP connection and route advertisement messages.

### Examples

```
-> ip bgp neighbor 172.22.2.115 admin-state enable
-> ip bgp neighbor 172.22.2.115 admin-state disable
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp neighbor**: Creates a BGP peer.
- **show ip bgp neighbors**: Displays peer parameters.

MIB Objects

- **alaBgpPeerTable**
- **alaBgpPeerAddr**
ip bgp neighbor advertisement-interval

Configures the time interval for updates between external BGP peers.

```
ip bgp neighbor ip_address advertisement-interval value
```

**Syntax Definitions**

- **ip_address**: 32-bit IP address of the neighbor.
- **value**: An advertisement time interval in seconds. The valid range is 0–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>30</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Internal peers sharing the same AS as the local BGP speaker (configured in the `ip bgp autonomous-system` command) use the global route advertisement update interval. This command sets the interval this peer uses to send BGP UPDATE messages to external peers.

**Examples**

````
-> ip bgp neighbor 172.22.2.115 255.255.255.0 advertisement-interval 60
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ip bgp neighbors*  
Displays BGP peer main status.

**MIB Objects**

alaBgpPeerTable

- alaBgpPeerAddr
- bgpPeerMinRouteAdvertisementTinterval
**ip bgp neighbor clear**

Restarts a BGP peer. The peer will be unavailable during this restart.

**Syntax Definitions**

`ip bgp neighbor ip_address clear`

- **ip_address**: 32-bit IP address of the neighbor.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command whenever changes occur to BGP-related access lists, weights, distribution lists, timer specifications, or administrative distance.

- Many peer commands restart the peer as soon as they are configured. The following commands restart the BGP peer for which they are configured:
  - `ip bgp neighbor remote-as`
  - `ip bgp neighbor md5 key`
  - `ip bgp neighbor passive`
  - `ip bgp neighbor ebgp-multihop`
  - `ip bgp neighbor maximum-prefix`
  - `ip bgp neighbor update-source`
  - `ip bgp neighbor next-hop-self`
  - `ip bgp neighbor soft-reconfiguration`
  - `ip bgp neighbor route-reflector-client`
  - `ip bgp confederation neighbor`
  - `ip bgp neighbor remove-private-as`
  - `ip bgp neighbor update-source`.

- You do not need to issue the **ip bgp neighbor clear** command after issuing any of the above commands.
**Examples**

-> ip bgp neighbor 172.22.2.115 clear

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**ip bgp neighbor auto-restart**  
Automatically attempts to restart a BGP peer session after a session terminates.

**MIB Objects**

alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerRestart
ip bgp neighbor route-reflector-client

Configures this peer as a client to the local route reflector.

ip bgp neighbor ip_address route-reflector-client
no ip bgp neighbor ip_address route-reflector-client

Syntax Definitions

ip_address 32-bit IP address of the neighbor.

Defaults

This command is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove this peer as a client to the local route reflector.
- This command configures this peer as one of the clients to the local route reflector.
- All of the peers configured using this command become part of the client group. The remaining peers are members of the non-client group for the local route reflector.
- When route reflection is configured, all of the internal BGP speakers in an autonomous system need not be fully meshed. The route reflector takes responsibility for passing internal BGP-learned routes to its peers.

Examples

-> ip bgp neighbor 172.22.2.115 route-reflector-client
-> no ip bgp neighbor 172.22.2.115 route-reflector-client

Release History

Release 7.1.1; command was introduced.
**Related Commands**

*ip bgp client-to-client reflection*  Configures the local BGP speaker as a route reflector

**MIB Objects**

*alaBgpPeerTable*
  - *alaBgpPeerAddr*
  - *alaBgpPeerClientStatus*
ip bgp neighbor default-originate

Enables or disables BGP peer default origination.

**ip bgp neighbor ip_address default-originate**

**no ip bgp neighbor ip_address default-originate**

### Syntax Definitions

*ip_address*  
32-bit IP address of the neighbor.

### Defaults

This command is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to disable this feature.

- When this command is enabled, the local BGP speaker advertises itself as a default to the peer. Such a default route overrides any learned default (propagation) and outbound policy. The default route 0.0.0.0 does not need to exist on the local router.

### Examples

-> ip bgp neighbor 172.22.2.115 default-originate

-> no ip bgp neighbor 172.22.2.115 default-originate

### Release History

Release 7.1.1; command was introduced.
Related Commands

**ip bgp neighbor**  Creates or deletes a BGP peer.

**MIB Objects**

- **alaBgpPeerTable**
  - **alaBgpPeerAddr**
  - **alaBgpPeerDefaultOriginate**
**ip bgp neighbor timers**

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified peer.

```
ip bgp neighbor ip_address timers keepalive holdtime
```

### Syntax Definitions

- `ip_address`: 32-bit IP address for the BGP peer.
- `keepalive`: The interval (in seconds) between KEEPALIVE messages. The valid values are zero (0) or the range 1–21845.
- `holdtime`: The hold time interval between updates to peers, in seconds. The valid range is 0, 3–65535.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>keepalive</td>
<td>30</td>
</tr>
<tr>
<td>holdtime</td>
<td>90</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Configures the time interval between KEEPALIVE messages sent by this peer. KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they serve only to tell the receiving BGP peer that the connection is still live and the peer is reachable.
- By default, the keep alive interval of 30 seconds is one-third the default hold-time interval of 90 seconds. The keep alive interval can never be more than one-third the value of the hold-time interval. When the hold interval is reached without receiving keep alive or other updates messages, the peer is considered dead.
- Setting the keep alive value to zero means no keep alive messages will be sent.
- Once a connection is established with a peer and a time period of the length specified in this command transpires with no messages from the remote peer, then the connection with that remote peer will be considered dead.
- Configures the tolerated hold time interval, in seconds, for messages to this peer from other peers. The hold timer is used during the connection setup process and in on-going connection maintenance with
BGP peers. If this peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.

- By default, the hold-interval of 180 seconds is three times the default keep-alive interval of 60 seconds. The hold-interval can never be less than three times the keep-alive value.
- You must restart the peer (using the `ip bgp neighbor clear` command) after issuing this command before the new hold time interval takes effect.
- Both values must be set at the same time.
- Entering this command without the variables resets the variables to their default value.

**Examples**

```
-> ip bgp neighbor 172.22.2.115 timers 80 240
-> ip bgp neighbor 172.22.2.115 timers
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`ip bgp neighbor conn-retry-interval`  
The interval, in seconds, between BGP retries to set up a connection through the transport protocol with another peer.

**MIB Objects**

`alaBgpPeerTable`  
`alaBgpPeerAddr`  
`bgpPeerHoldTimeConfigured`  
`bgpPeerKeepAliveConfigured`
**ip bgp neighbor conn-retry-interval**

The interval, in seconds, between BGP retries to set up a connection through the transport protocol with another peer. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connect retry interval is started. Once this interval elapses, BGP retries setting up the connection.

```
ip bgp neighbor ip_address conn-retry-interval seconds
```

**Syntax Definitions**

- `ip_address`: 32-bit IP address for the neighbor.
- `seconds`: The time interval (in seconds) between retries. The valid range is 0–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>120</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The time interval is started when a connection to a peer is lost.
- Other BGP peers may automatically attempt to restart a connection with this peer if they have configured automatic peer session restart (using the `ip bgp neighbor auto-restart` command).
- You must restart the peer (using the `ip bgp neighbor clear` command) after issuing this command before the new connection retry interval takes effect.
- Entering this command without the `seconds` variable resets the variable to its default value.

**Examples**

- `-> ip bgp neighbor 172.22.2.115 connect-interval 60`
- `-> ip bgp neighbor 172.22.2.115 connect-interval`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `ip bgp neighbor auto-restart`: Enable automatic session restart after a session termination.
- `ip bgp neighbor clear`: Restarts the peer.

MIB Objects

- `alaBgpPeerTable`
  - `alaBgpPeerAddr`
  - `bgpPeerConnectRetryInterval`
ip bgp neighbor auto-restart

Enables or disables BGP peer automatic restart. When enabled, this peer will automatically attempt to restart a session with another peer after a session with that peer terminates. When disabled, this peer will not try to re-establish a session with another peer after the session terminates; in such a case, the other peer will have to restart the session for the two peers to resume communication.

**ip bgp neighbor ip_address auto-restart**

**Syntax Definitions**

| ip_address | 32-bit IP address for the neighbor. |

**Defaults**

This command is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the no form of this command to disable automatic peer restart.

- After a session with another peer terminates, the local BGP speaker will wait 60 seconds before attempting to restart the session. If the session does not start on the first attempt a second attempt will be made after another 120 seconds (60x2). On each unsuccessful session attempt, the previous delay between restarts is multiplied by 2, up to a maximum delay of 240 seconds. An exception to this rule occurs when the peer session terminates on receipt of a NOTIFY message with 'unsupported option' code or 'unsupported capability' code; in these cases the delay between restart attempts will begin at 1 second and multiply by 2 after each unsuccessful restart attempt (up to a maximum of 240 second delay).

- Disabling this option can be helpful in cases where other peers are prone to frequent flapping or sending many NOTIFY messages. By not restarting sessions with unstable neighbors, the local BGP speaker forces those unstable neighbors to re-initialize the connection.

**Examples**

```bash
-> ip bgp neighbor 172.22.2.115 auto-restart
-> no ip bgp neighbor 172.22.2.115 auto-restart
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

`ip bgp neighbor` Creates a BGP peer.

`ip bgp neighbor admin-state` Enables a BGP peer.

**MIB Objects**

- `alaBgpPeerTable`
  - `alaBgpPeerAddr`
  - `alaBgpPeerAutoRestart`
ip bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from this peer in UPDATE messages.

**ip bgp neighbor ip_address maximum-prefix maximum [warning-only]**

---

**Syntax Definitions**

- **ip_address**: 32-bit IP address for the BGP peer.
- **maximum**: The maximum number of prefixes. The valid range is 0–4294967295.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>5000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the number of prefixes sent by this peer reaches this limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from this peer reaches 80 percent of the value you configure in this command.
- If the **warning-only** prefix is used, the operator will be warned when the peer exceeds 80 percent of the configured number of maximum prefixes.
- The BGP peer is restarted after issuing this command.

**Examples**

```bash
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000
-> ip bgp neighbor 172.22.2.115 maximum-prefix 1000 warning only
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

```markdown
**ip bgp neighbor clear**
Restarts the BGP peer.
```

MIB Objects

```markdown
alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerMaxPrefixWarnOnly
  alaBgpPeerMaxPrefix
```
ip bgp neighbor md5 key

Sets an encrypted MD5 signature for TCP sessions with this peer in compliance with RFC 2385.

ip bgp neighbor ip_address md5 key {string | none}

Syntax Definitions

- **ip_address**: 32-bit IP address of the BGP peer.
- **string**: The MD5 public key. Maximum character length is 200.
- **none**: Removes the MD5 public key.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>no password</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Entering the keyword **none** in place of a key removes the password and disables authentication.

- Due to security concerns the actual password that you specify in this command is encrypted using a 3DES algorithm before it appears in a saved snapshot file. Also, if you were to view this command in a snapshot file, or **boot.cfg** file, it would appear in a different syntax. The syntax for this command used in snapshot files is as follows:

  **ip bgp neighbor ip_address md5 key-encrypt encrypted_string**

  However, you should not use this syntax to actually set an MD5 password; it will not work.

- The BGP peer is restarted after issuing this command.

Examples

-> ip bgp neighbor 172.22.2.115 md5 key openpeer5

Release History

Release 7.1.1; command was introduced.
**Related Commands**

**ip bgp neighbor clear**

Restarts the BGP peer.

**MIB Objects**

alaBgpPeerTable

alaBgpPeerAddr
alaBgpPeerMD5Key
ip bgp neighbor ebgp-multihop

Allows external peers to communicate with each other even when they are not directly connected. The absence of communication between disconnected peers can occur when a router that is not running BGP sits between two BGP speakers; in such a scenario the BGP speakers are multiple hops from each other. By enabling this command, you allow the BGP peers to speak to each other despite the non-BGP router that sits between them.

ip bgp neighbor ip_address ebgp-multihop [ttl]
no ip bgp neighbor ip_address ebgp-multihop

Syntax Definitions

- **ip_address**: 32-bit IP address of the BGP peer.
- **ttl**: The Time to Live for the multi-hop connection, in seconds. The range is 1 to 255.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ttl</td>
<td>255</td>
</tr>
</tbody>
</table>

This command is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to disable multi-hop connections.
- By default an external BGP peer is on a directly connected subnet. This command allows you to configure an external BGP peer that is not directly connected and may be multiple hops away. It should be used with caution and only with the guidance of qualified technical support.
- As a safeguard against loops, the multi-hop connection will not be made if the only route to a multi-hop peer is the default route (0.0.0.0).
- The BGP peer is restarted after issuing this command.
- When eBGP multihop is enabled, GTSM must be disabled or vice-versa.
Examples

-> ip bgp neighbor 172.22.2.115 ebgp-multihop 250
-> no ip bgp neighbor 172.22.2.115 ebgp-multihop 50

Release History

Release 7.1.1; command was introduced.

Related Commands

- **ip bgp neighbor**  
  Creates or deletes a BGP peer.
- **ip bgp neighbor next-hop-self**  
  Sets the BGP peer to use next hop processing behavior.

MIB Objects

- **alaBgpPeerTable**
  - **alaBgpPeerAddr**
  - **alaBgpPeerMultiHop**
### ip bgp neighbor description

Configures the BGP peer name.

```plaintext
ip bgp neighbor ip_address description string
```

#### Syntax Definitions

- `ip_address` 32-bit IP address of the BGP peer.
- `string` Peer name (1–20 characters).

#### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>string</code></td>
<td>peer(ip_address)</td>
</tr>
</tbody>
</table>

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- The peer name is a text identifier that, by default, follows the format “peer(x.x.x.x)” where x.x.x.x is the IP address of the BGP peer. For example, the default name of a peer at address 198.216.14.23 would be “peer(198.216.14.23)”.
- A peer name with embedded spaces must be enclosed in quotation marks.

#### Examples

```plaintext
-> ip bgp neighbor 172.22.2.115 description "peer for building 3"
```

#### Release History

Release 7.1.1; command was introduced.

#### Related Commands

- `ip bgp neighbor` Sets the IP address for the peer.

#### MIB Objects

- `alaBgpPeerTable`
- `alaBgpPeerAddr`
alaBgpPeerName
ip bgp neighbor next-hop-self

Sets the BGP peer to use next hop processing behavior. By default, the next-hop processing of BGP updates is disabled. Using this command to enable next-hop behavior may be useful in non-meshed networks where BGP peers do not have direct access to other peers.

`ip bgp neighbor ip_address next-hop-self`

`no ip bgp neighbor ip_address next-hop-self`

---

**Syntax Definitions**

N/A

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable next hop processing behavior.

- In partially meshed networks a BGP peer may not have direct connections to other peers. When such a peer receives route updates from these distant peers (through other peers), it may treat the remote peer as if it were the next hop in the routing path. Packet forwarding will not work in such a case because no direct connection exists. This command allows this peer to deem itself the next hop on the routing path so that the two non-connected peers can route packets. This peer would have a direct connection to both peers that want to exchange packets.

- The BGP peer is restarted after issuing this command.

**Examples**

`-> ip bgp neighbor 172.22.2.115 next-hop-self`

`-> no ip bgp neighbor 172.22.2.115 next-hop-self`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ip bgp neighbor**  Creates or deletes a BGP peer.

MIB Objects

alaBgpPeerTable
- alaBgpPeerAddr
- alaBgpPeerNextHopSelf
ip bgp neighbor passive

Configures the local BGP speaker to wait for this peer to establish a connection. When enabled, the local BGP speaker will not initiate a peer session with this peer; in this sense, the BGP speaker is “passive.” When disabled, the local BGP speaker will attempt to set up a session with this peer.

ip bgp neighbor ip_address passive

no ip bgp neighbor ip_address passive

Syntax Definitions

ip_address 32-bit IP address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable passive peer behavior.
- By default BGP will initiate a session to a peer once the peer is configured, has an AS number, and is enabled. You can use this command to configure the local BGP speaker as passive and an outbound session will not be initiated to this peer. For such peers, BGP will always wait passively for the inbound session attempt.
- The BGP peer is restarted after issuing this command.

Examples

-> ip bgp neighbor 172.22.2.115 passive
-> no ip bgp neighbor 172.22.2.115 passive

Release History

Release 7.1.1; command was introduced.
Related Commands

**ip bgp neighbor**
Creates or deletes a BGP peer.

MIB Objects

*alaBgpPeerTable*
  *alaBgpPeerAddr*
  *alaBgpPeerPassive*
**ip bgp neighbor remote-as**

Assigns an AS number to this BGP peer.

`ip bgp neighbor ip_address remote-as value`

### Syntax Definitions

- `ip_address`: 32-bit IP address of the BGP peer.
- `value`: Autonomous system number in the asplain, asdot+, or asdot formats.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- A BGP peer created with the `ip bgp neighbor` command cannot be enabled (**ip bgp neighbor admin-state enable**) until it is assigned an autonomous system number. If the AS number matches the AS number assigned to the local BGP speaker (assigned using the `ip bgp autonomous-system` command), the peer is considered internal to the local autonomous system. Otherwise, the peer is consider external to the local BGP speaker’s AS.
- This BGP peer may not be operational within this router and it may be in an external AS, but it must still be configured on this router before the local BGP speaker can establish a connection to the peer. The local BGP speaker does not auto-discover peers in other routers; it initially learns about peers through the peer commands.
- The BGP peer is restarted after issuing this command.
- The 4-octet ASN is represented in one of three ways:
  - asplain (simple decimal notation)
  - asdot+ (two 16-bit values as low-order and high-order)
  - asdot (a mixture of asplain and asdot+).
**Examples**

-> ip bgp neighbor 172.22.2.115 remote-as 100

The following examples show how to configure the BGP neighbor ASN as 65535 in the three different formats:

-> ip bgp neighbor 2.2.2.2 remote-as 65535        (asplain format)
-> ip bgp neighbor 2.2.2.2 remote-as 0.65535      (asdot+ format)
-> ip bgp neighbor 2.2.2.2 remote-as 65535        (asdot format)

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.3; support for 4-octet ASN was added.

**Related Commands**

- **ip bgp autonomous-system** Set the AS for the local BGP speaker.
- **ip bgp neighbor** Create a BGP peer.
- **ip bgp neighbor admin-state enable** Enables a BGP peer.

**MIB Objects**

alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerAS
**ip bgp neighbor remove-private-as**

Enables or disables the stripping of private autonomous system numbers from the AS path of routes destined to this peer.

```plaintext
ip bgp neighbor ip_address remove-private-as
no ip bgp neighbor ip_address remove-private-as
```

**Syntax Definitions**

*ip_address*  
32-bit IP address of the BGP peer.

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to disable stripping of private AS numbers.
- By default all AS numbers in the AS path are passed to peers. Enabling this command strips any private AS numbers in the AS path before sending updates to this peer. AS numbers in the range 64512 to 65535 are considered private ASs; they intended for internal use within an organization (such as an enterprise network), but they are not intended for use on public networks (such as the Internet).
- This command has no effect if you are not using ASs in the range 64512 to 65535.
- The BGP peer is restarted after issuing this command.

**Examples**

```plaintext
-> ip bgp neighbor 172.22.2.115 remove-private-as
-> no ip bgp neighbor 172.22.2.115 remove-private-as
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

`ip bgp neighbor remote-as`  Configures the AS number for this peer.

MIB Objects

alaBgpPeerTable
- alaBgpPeerAddr
- alaBgpPeerRemovePrivateAs
**ip bgp neighbor soft-reconfiguration**

Enables or disables BGP peer soft reconfiguration. Soft reconfiguration increases the stability of the peer by allowing you to reconfigure attributes that require peer resets without halting the TCP connection with other peers.

```
ip bgp neighbor ip_address soft-reconfiguration
no ip bgp neighbor ip_address soft-reconfiguration
```

**Syntax Definitions**

*ip_address* 32-bit IP address of the BGP peer.

**Default**

This command is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to disable this feature.
- This feature stores routes and other configuration information in local memory. When you make configuration changes that require a peer reset, the routing cache is not cleared and connections with other peers are not interrupted.
- If a peer is not route-refresh capable, by default, BGP stores all paths from peers, even those that are policy rejected, in anticipation of policy changes in the future. Storing these paths consumes memory. You can use this command to disable the storing of these paths, or soft reconfiguration. However, if soft reconfiguration is disabled and the peer is not route-refresh capable and the inbound policy changes, the peer will have to be restarted using the *ip bgp neighbor clear* command.
- If the peer is route-refresh capable and soft reconfiguration is disabled, inbound policy changes are still supported without re-starting the peer.

**Examples**

```
-> ip bgp neighbor 172.22.2.115 soft-reconfiguration
-> no ip bgp neighbor 172.22.2.115 soft-reconfiguration
```
BGP Commands

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bgp neighbor clear** Reverts this BGP peer.
- **ip bgp neighbor clear soft** Invokes an inbound or outbound policy reconfiguration for a BGP peer.

**MIB Objects**

- **alaBgpPeerTable**
  - **alaBgpPeerAddr**
  - **alaBgpPeerSoftReconfig**
**ip bgp neighbor stats-clear**

Clears the statistics for a peer.

`ip bgp neighbor ip_address stats-clear`

**Syntax Definitions**

`ip_address` 32-bit IP address of the BGP peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command clears the statistical variables for a peer so they can accumulate from a known point.

- The cleared statistics include the total messages sent and received from this peer, the total UPDATE messages sent and received from this peer, the total NOTIFY messages sent and received from this peer, and the total peer state transition messages sent and received from this peer. These statistics can be displayed through `show ip bgp neighbors statistics`.

**Examples**

`-> ip bgp neighbor 172.22.2.115 stats-clear`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`show ip bgp neighbors statistics` Displays peer statistics.

**MIB Objects**

alaBgpPeerTable
  alaBgpPeerAddr
  alaBgpPeerClearCounter
**ip bgp confederation neighbor**

Configures this peer as a member of the same confederation as the local BGP speaker.

**ip bgp confederation neighbor** *ip_address*

**no ip bgp confederation neighbor** *ip_address*

---

**Syntax Definitions**

*ip_address* 32-bit IP address of the BGP peer.

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes/Deterministic</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to disable this feature.
- You must first assign a confederation number to the local BGP speaker before assigning peers to the confederation. Use the **ip bgp confederation identifier** command to assign a confederation number to the local BGP speaker.
- The BGP peer is restarted after issuing this command.

**Examples**

- `-> ip bgp confederation neighbor 172.22.2.115`
- `-> no ip bgp confederation neighbor 172.22.2.115`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bgp confederation identifier** Sets a confederation identification value for the local BGP speaker (this router).

**MIB Objects**

- `alaBgpPeerTable`
- `alaBgpPeerAddr`
alaBgpPeerConfedStatus
ip bgp neighbor update-source

Configures the local address from which this peer will be contacted. This local address can be configured for internal and external BGP peers.

`ip bgp neighbor ip_address update-source [interface_name]`

### Syntax Definitions

- `ip_address` 32-bit IP address of the BGP peer.
- `interface_name` The name of the interface.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface_address</code></td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This address does not override the router identification for this BGP peer (configured in the `ip bgp neighbor` command). It is the address through which this peer can be contacted within this router. The router identification for a peer, especially an external peer, may not exist in the local router, but that distant peer can still be contacted through this router. This command sets the local address through which this distant peer can be contacted.
- The default is restored by entering the command without a IP address.
- The BGP peer is restarted after issuing this command.
- The update-source is not related to the router-id, it specifies the interface to be used for the TCP connection endpoint. By default, the nearest interface is selected.

### Examples

- `-> ip bgp neighbor 172.22.5.115 update-source 172.22.2.117`
- `-> ip bgp neighbor 172.22.5.115 update-source vlan-22`
- `-> ip bgp neighbor 172.22.5.115 update-source`
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bgp neighbor**

  Sets the router identification for a BGP peer.

**MIB Objects**

- **alaBgpPeerTable**
  - **alaBgpPeerAddr**
  - **alaBgpPeerLocalAddr**
  - **alaBgpPeerLocalIntfName**
ip bgp neighbor in-aspathlist

Assigns an inbound AS path list filter to a BGP peer.

\texttt{ip bgp neighbor ip\_address in-aspathlist \{string | none\}}

**Syntax Definitions**

- \texttt{ip\_address} \hspace{1cm} 32-bit IP address of the BGP peer.
- \texttt{string} \hspace{1cm} Inbound AS path list (0 to 70 characters). This name is case sensitive.
- \texttt{none} \hspace{1cm} Removes this AS path list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The AS path list name (\texttt{InboundASpath} in the example below) is created using the \texttt{ip bgp policy aspath-list} command. Any inbound routes from the BGP peer must match this AS path filter before being accepted or passed to inbound policy.
- To deassign an input AS path filter list, use this command to assign a value of \texttt{none}.

**Examples**

- \texttt{-> ip bgp neighbor 172.22.2.115 in-aspathlist InboundASPath}
- \texttt{-> ip bgp neighbor 172.22.2.115 in-aspathlist none}

**Release History**

Release 7.1.1; command was introduced.
Related Commands

ip bgp policy aspath-list  Creates or removes an AS path list.

MIB Objects

alaBgpPeerTable
  alaBgpPeerAspathListIn
**ip bgp neighbor in-communitylist**

Assigns an inbound community list filter to a BGP peer.

```
ip bgp neighbor ip_address in-communitylist {string | none}
```

### Syntax Definitions

- **ip_address**: 32-bit IP address of the BGP peer.
- **string**: Input community list (0 to 70 characters). This name is case sensitive.
- **none**: Removes this community list from the peer.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The community filter list name (**InboundCommlist** in the example below) is created using the `ip bgp policy community-list` command. Any inbound routes from the BGP peer must match this community filter before being accepted or passed to inbound policy.

- To deassign an input community filter list, use this command to assign a value of “**none**.”

### Examples

```
-> ip bgp neighbor 172.22.2.115 in-communitylist InboundCommlist
-> ip bgp neighbor 172.22.2.115 in-communitylist none
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

*ip bgp policy community-list*  Creates or deletes a community list.

MIB Objects

alaBgpPeerTable
  
  alaBgpPeerCommunityListIn
**ip bgp neighbor in-prefixlist**

Assigns an inbound prefix filter list to a BGP peer.

```bash
ip bgp neighbor ip_address in-prefixlist {string | none}
```

### Syntax Definitions

- **ip_address**: 32-bit IP address of the BGP peer.
- **string**: Input prefix filter list (0 to 70 characters). This name is case sensitive.
- **none**: Removes this prefix list from the peer.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The prefix list name (**InboundPrefix** in the example below) is created using the `ip bgp policy prefix-list` command. Any inbound routes from the BGP peer must match this prefix filter before being accepted or passed to inbound policy.
- To deassign an input prefix filter list, use this command to assign a value of **“none.”**

### Examples

- `-> ip bgp neighbor 172.22.2.115 in-prefixlist InboundPrefix`
- `-> ip bgp neighbor 172.22.2.115 in-prefixlist none`

### Release History

Release 7.1.1; command was introduced.
Related Commands

`ip bgp policy prefix-list` Creates or deletes a prefix match list.

MIB Objects

alaBgpPeerTable
  alaBgpPeerPrefixListIn
**ip bgp neighbor in-prefix6list**

Assigns an inbound prefix6 list to a BGP peer.

`ip bgp neighbor ip_address in-prefix6list {string | none}`

---

### Syntax Definitions

- **ip_address**: 32-bit IP address of the BGP peer.
- **string**: Input prefix6 filter list (0 to 70 characters). This name is case sensitive.
- **none**: Removes this prefix6 list from the peer.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The prefix6 list name (**InboundPrefix6** in the example below) is created using the `ip bgp policy prefix6-list` command. Any inbound IPv6 routes from the BGP peer must match this prefix6 filter before being accepted or passed to inbound policy.
- To deassign an input prefix6 filter list, use this command to assign a value of “**none**.”

### Examples

- `-> ip bgp neighbor 172.22.2.115 in-prefix6list InboundPrefix6`
- `-> ip bgp neighbor 172.22.2.115 in-prefix6list none`

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

*ip bgp policy prefix6-list*  
Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

**MIB Objects**

*alaBgpPeerTable*  
*alaBgpPeerPrefix6ListIn*
**ip bgp neighbor out-aspathlist**

Assigns an outbound AS path filter list to a BGP peer.

```
ip bgp neighbor ip_address out-aspathlist {string | none}
```

### Syntax Definitions

- **ip_address**: 32-bit IP address of the BGP peer.
- **string**: Outbound AS path list (0 - 70 characters).
- **none**: Removes the AS path list from the peer.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The AS path list name (OutboundASPath in the example below) is created using the `ip bgp policy aspath-list` command. Any outbound routes from the BGP peer must match this AS path filter, or policy, before being advertised or passed to outbound policy.

- To deassign an output AS path filter list, use this command to assign a value of “none”.

### Examples

```
-> ip bgp neighbor 172.22.2.115 out-aspathlist OutboundASPath
-> ip bgp neighbor 172.22.2.115 out-aspathlist none
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

*ip bgp policy aspath-list* Creates or removes an AS path list.

**MIB Objects**

alaBgpPeerTable

- alaBgpPeerAspathListOut
**ip bgp neighbor out-communitylist**

Assigns an outbound community filter list to a BGP peer.

```
ip bgp neighbor ip_address out-communitylist {string | none}
```

**Syntax Definitions**

- `ip_address` 32-bit IP address of the BGP peer.
- `string` Outbound community list (0 - 70 characters).
- `none` Removes the community list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The community filter list name (**OutboundCommlist** in the example below) is created using the `ip bgp policy community-list` command. Any outbound routes from the BGP peer must match this community filter before being advertised or passed to outbound policy.

- To deassign an output community filter list, use this command to assign a value of “none”.

**Examples**

```
-> ip bgp neighbor 172.22.2.115 out-communitylist OutboundCommlist
-> ip bgp neighbor 172.22.2.115 out-communitylist none
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

`ip bgp policy community-list`  Creates or deletes a community list.

MIB Objects

`alaBgpPeerTable`
  `alaBgpPeerCommunityListOut`
### ip bgp neighbor out-prefixlist

Assigns an outbound prefix filter list to a BGP peer.

```
ip bgp neighbor ip_address out-prefixlist {string | none}
```

#### Syntax Definitions

- **ip_address**: 32-bit IP address of the BGP peer.
- **string**: Output prefix filter list (0 - 70 characters).
- **none**: Removes the prefix list from the peer.

#### Defaults

N/A

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- The prefix list name (**OutboundPrefix** in the example below) is created using the `ip bgp policy prefix-list` command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to outbound policy.
- To deassign an output prefix filter list, use this command to assign a value of “**none**”.

#### Examples

```
-> ip bgp neighbor 172.22.2.115 out-prefixlist OutboundPrefix
-> ip bgp neighbor 172.22.2.115 out-prefixlist none
```

#### Release History

Release 7.1.1; command was introduced.
**Related Commands**

`ip bgp policy prefix-list`  Creates or deletes a prefix match list.

**MIB Objects**

`alaBgpPeerTable`
  `alaBgpPeerPrefixListOut`
ip bgp neighbor out-prefix6list

Assigns an outbound prefix6 filter list to a BGP peer.

`ip bgp neighbor ip_address out-prefix6list {string | none}`

**Syntax Definitions**

- `ip_address` 32-bit IP address of the BGP peer.
- `string` Output prefix6 filter list (0 - 70 characters).
- `none` Removes the prefix6 list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The prefix6 list name (OutboundPrefix6 in the example below) is created using the `ip bgp policy prefix6-list` command. Any outbound IPv6 routes from the BGP peer must match this prefix6 filter before being advertised or passed to outbound policy.
- To deassign an output prefix6 filter list, use this command to assign a value of “none”.

**Examples**

- `-> ip bgp neighbor 172.22.2.115 out-prefix6list OutboundPrefix6`
- `-> ip bgp neighbor 172.22.2.115 out-prefix6list none`

**Release History**

Release 7.1.1; command was introduced.
BGP Commands

ip bgp neighbor out-prefix6list

Related Commands

ip bgp policy prefix6-list Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

alaBgpPeerTable
  alaBgpPeerPrefix6ListOut
**ip bgp neighbor route-map**

Assigns a policy map (inbound or outbound) to a BGP peer.

```
ip bgp neighbor ip_address route-map {string | none} {in | out}
oip bgp neighbor ip_address route-map {in | out}
```

**Syntax Definitions**

- `ip_address` 32-bit IP address of the peer.
- `string` Policy map name (0 to 70 characters). This name is case sensitive.
- `none` Deletes the route map if entered rather than a text string.
- `in` Designates this route map policy as an inbound policy.
- `out` Designates this route map policy as an outbound policy.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to deassign an inbound or an outbound policy.
- The policy route map name (**InboundRoute** in the example below) is created using the `ip bgp policy route-map` command. Any inbound routes from the BGP peer must match this route map filter before being accepted or passed to inbound policy.
- The policy route map name (**OutboundRoute** in the example below) is created using the `ip bgp policy route-map` command. Any outbound routes for the BGP peer must match this route map filter before being advertised or passed to outbound policy.
- It is also possible to deassign a route map by entering `none` in place of a route map name.

**Examples**

```
-> ip bgp neighbor 172.22.2.115 route-map InboundRoute in
-> ip bgp neighbor 172.22.2.115 route-map OutboundRoute out
-> ip bgp neighbor 172.22.2.115 route-map none in
-> no ip bgp neighbor 172.22.2.115 route-map in
```
Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map

Creates or deletes a policy route map.

MIB Objects

alaBgpPeerTable
  alaBgpPeerRouteMapOut
  alaBgpPeerRouteMapIn
**ip bgp neighbor clear soft**

Invokes an inbound or outbound policy reconfiguration for a BGP peer.

```
ip bgp neighbor ip_address clear soft {in | out}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_address</code></td>
<td>32-bit IP address of the BGP peer.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies reconfiguration to the inbound policies.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies reconfiguration to the outbound policies.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command reconfigures (or reapplies) all inbound or outbound policies to existing routes without restarting the peer session.
- This command is useful if policies have been changed.

### Examples

```
-> ip bgp neighbor 172.22.2.115 clear soft in
-> ip bgp neighbor 172.22.2.115 clear soft out
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `ip bgp neighbor soft-reconfiguration` Enables or disables BGP peer soft reconfiguration.

### MIB Objects

- `alaBgpPeerTable`
- `alaBgpPeerReconfigureInBound`
BGP Commands

ip bgp neighbor clear soft

alaBgpPeerReconfigureOutBound
bgp neighbor check-first-as

Configures the check for the first AS in the ASPATH list while processing UPDATE message from BGP neighbor.

```bash
{ip | ipv6} bgp neighbor {ipv4_address | ipv6_address} check-first-as
no {ip | ipv6} bgp neighbor {ipv4_address | ipv6_address} check-first-as
```

**Syntax Definitions**

- `ipv4_address | ipv6_address`: IPv4 or IPv6 address of the BGP neighbor based on the IP address type selected.

**Defaults**

By default, the first AS in the ASPATH list will be checked.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `ip` keyword to configure the check for the first AS in the ASPATH from an IPv4 BGP neighbor.
- Use the `ipv6` keyword to configure the check for the first AS in the ASPATH from an IPv6 BGP neighbor.
- Use the `no` form of the command to remove the check for the first AS in the ASPATH list while processing an update message from BGP neighbor.

**Examples**

- `ip bgp neighbor 172.22.2.115 check-first-as`
- `ipv6 bgp neighbor fe80::2efa:a2ff:fe13:e402 check-first-as`
- `no ip bgp neighbor 172.22.2.115 check-first-as`
- `no ipv6 bgp neighbor fe80::2efa:a2ff:fe13:e402 check-first-as`

**Release History**

Release 8.7 R1; command was introduced.
**Related Commands**

- `show ip bgp neighbors` Displays the configured IPv4 BGP peers.
- `show ipv6 bgp neighbors` Displays the configured IPv6 BGP peers.

**MIB Objects**

- `alaBgpPeerTable`
  - `alaBgpPeerCheckFirstAS`
  - `alaBgpPeer6CheckFirstAS`
**ip bgp bfd-state**

Enables or disables the registration of BGP with the BFD protocol.

`ip bgp bfd-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for BGP.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for BGP.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- BFD must be globally enabled for the switch and BGP must be registered with BFD at the protocol level before BGP can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and the BGP protocol acts based upon the BFD message.
- Whenever a neighbor goes down, BGP will inform BFD to remove that neighbor from the BFD active list.

**Examples**

Globally enables the BFD protocol for the switch:

`-> ip bfd admin-state enable`

Enables and disables the registration of BGP with the BFD protocol:

`-> ip bgp bfd-state enable`

`-> ip bgp bfd-state disable`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip bfd admin-state**: Enables or disables the global BFD protocol status for the switch.
- **ip bgp bfd-state all-neighbors**: Enables or disables BFD for all BGP neighbors.
- **ip|ipv6 bgp neighbor bfd-state**: Enables or disables BFD for a specific neighbor.
- **show ip bgp**: Displays the current global settings for the local BGP speaker.

MIB Objects

- **alaBgpGlobal**
  - **alaBgpBfdStatus**
**ip bgp bfd-state all-neighbors**

Enables or disables BFD for all BGP neighbors.

```plaintext
ip bgp bfd-state all-neighbors {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for all the BGP neighbors.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for all the BGP neighbors.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BFD status for BGP must be enabled before BGP can interact with BFD.

**Examples**

```plaintext
-> ip bgp bfd-state all-neighbors enable
-> ip bgp bfd-state all-neighbors disable
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `bgp neighbor check-first-as` Enables or disables BGP with BFD protocol.
- `ip|ipv6 bgp neighbor bfd-state` Enables or disables the BFD for a specific BGP neighbor.
- `show ip bgp neighbors` Displays the configured IPv4 BGP peers.

**MIB Objects**

- `alaBgpGlobal` alaBgpBfdAllNeighbors
**ip|ipv6 bgp neighbor bfd-state**

Enables or disables BFD for a specific IPv4 or IPv6 BGP neighbor.

```
{ip | ipv6} bgp neighbor {ipv4_address | ipv6_address} bfd-state {enable | disable}
```

### Syntax Definitions

- `ipv4_address`: The IPv4 address of the BGP neighbor.
- `ipv6_address`: The IPv6 address of the BGP neighbor.
- `enable`: Enables BGP neighbor.
- `disable`: Disables BGP neighbor.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The BFD status for BGP must be enabled before BGP can interact with BFD.

### Examples

- `-> ip bgp neighbor 135.10.10.2 bfd-state enable`
- `-> ip bgp neighbor 135.10.10.2 bfd-state disable`

- `-> ipv6 bgp neighbor fe80::2efa:a2ff:fe13:e402 bfd-state enable`
- `-> ipv6 bgp neighbor fe80::2efa:a2ff:fe13:e402 bfd-state disable`

### Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R03; IPv6 BFD support added.
**Related Commands**

- `bgp neighbor check-first-as` Enables or disables BGP with BFD protocol.
- `ip bgp bfd-state all-neighbors` Enables or disables BFD for all BGP neighbors.
- `show ip bgp neighbors` Displays the configured IPv4 BGP peers.

**MIB Objects**

- `alaBgpPeerEntry`  
  - `alaBgpPeerName`  
  - `alaBgpPeerBfdStatus`  
- `alaBgpGlobal`  
  - `alaBgpBfdAllNeighbors`
**ip bgp policy aspath-list**

Creates or removes an AS path list.

**ip bgp policy aspath-list name “regular_expression”**

**no ip bgp policy aspath-list name “regular_expression”**

---

**Syntax Definitions**

*name*  
AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.

*regular_expression*  
Regular expression, for example, “^100 200$” where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.

---

**Defaults**

No IP BGP peer policy AS path-list exists.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to remove an AS path list.
- To create an AS path list, use the **ip bgp policy aspath-list** command.
- A regular expression consists of a character string presented in the form of a pattern, e.g., “^100 200$.” Valid regular expression characters (metacharacters) are shown in the table below. See also “Configuring BGP” in your Advanced Routing Guide for more information on using regular expressions in BGP commands.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Matches the beginning of the AS path list.</td>
</tr>
<tr>
<td>123</td>
<td>Matches the AS number 123.</td>
</tr>
<tr>
<td>.</td>
<td>Matches any single AS number.</td>
</tr>
<tr>
<td>?</td>
<td>Matches zero or one occurrence of the previous token, which must be an AS number, a dot, an alternation or a range.</td>
</tr>
<tr>
<td>+</td>
<td>Matches one or more occurrences of the previous token, which must be an AS number, a dot, an alternation or a range.</td>
</tr>
</tbody>
</table>
When using a regular expression in the CLI, the regular expression must be enclosed in quotation marks.

This command creates AS path lists that can be applied to a peer’s inbound and outbound routes using the `ip bgp neighbor in-aspathlist`, `ip bgp neighbor out-aspathlist`, `ipv6 bgp neighbor in-aspathlist`, and `ipv6 bgp neighbor out-aspathlist` commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the `permit` or `deny` action (i.e., policy) associated with the regular expression applies.

If a BGP AS path list is configured to deny routes from a particular string of regular expression, then by default all of the routes coming from any AS would be denied. You must configure the policy instance in the same policy to allow other routes to come in, to be permitted from other ASs.

General or more specific AS path list information can be displayed by varying the use of the `show ip bgp policy aspath-list` command.

**Examples**

- `-> ip bgp policy aspath-list InboundAspath "^100 200$"`
- `-> ip bgp policy aspath-list OutboundAspath "^300 400$"`
- `-> no ip bgp policy aspath-list InboundAspath "^100 200$"

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip bgp neighbor in-aspathlist` Assigns an inbound AS path list filter to a BGP peer.
- `ip bgp neighbor out-aspathlist` Assigns an outbound AS path list filter to a BGP peer.
- `ip bgp policy aspath-list action` Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found.
- `ip bgp policy aspath-list priority` Configures priority for processing regular expressions in an AS path list.
- `ipv6 bgp neighbor in-aspathlist` Assigns an inbound AS path list filter to an IPv6 BGP peer.
- `ipv6 bgp neighbor out-aspathlist` Assigns an outbound AS path filter list to an IPv6 BGP peer.

**MIB Objects**

- `alaBgpAspathMatchListTable`  
  - `alaBgpAspathMatchListRowStatus`
ip bgp policy aspath-list action

Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found. Matching criteria are specified in the regular expression.

```
ip bgp policy aspath-list name "regular_expression" action {permit | deny}
```

### Syntax Definitions

- **name**: AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
- **regular_expression**: Regular expression, e.g., “^100 200$” where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
- **permit**: Allows matching routes to pass.
- **deny**: Stops matching routes from passing.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Examples

-> ip bgp policy aspath-list InboundAspath "^100 200$" action permit
-> ip bgp policy aspath-list OutboundAspath "^300 400$" action deny

Release History

Release 7.1.1; command was introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip bgp neighbor in-aspathlist</td>
<td>Assigns an inbound AS path list filter to a BGP peer.</td>
</tr>
<tr>
<td>ip bgp neighbor out-aspathlist</td>
<td>Assigns an outbound AS path list filter to a BGP peer.</td>
</tr>
<tr>
<td>ip bgp policy aspath-list</td>
<td>Creates or removes an AS path list.</td>
</tr>
<tr>
<td>ip bgp policy aspath-list priority</td>
<td>Configures priority for processing regular expressions in an AS path list.</td>
</tr>
<tr>
<td>ipv6 bgp neighbor in-aspathlist</td>
<td>Assigns an inbound AS path list filter to an IPv6 BGP peer.</td>
</tr>
<tr>
<td>ipv6 bgp neighbor out-aspathlist</td>
<td>Assigns an outbound AS path filter list to an IPv6 BGP peer.</td>
</tr>
</tbody>
</table>

MIB Objects

alaBgpAspathMatchListTable
alaBgpAspathMatchListAction
ip bgp policy aspath-list priority

Configures the priority for processing regular expressions in an AS path list.

```
ip bgp policy aspath-list name "regular_expression" priority value
```

**Syntax Definitions**

- **name**: AS path name, e.g., InboundAspath, ranging from 0 to 70 characters, or a value of none. The AS path name is case sensitive.
- **regular_expression**: Regular expression, e.g., “^100 200$” where 100 (followed by a space) represents the beginning of the list and 200 represents the end. The regular expression must be enclosed by quotation marks.
- **value**: A priority value, e.g., 1, assigned to the policy action. Valid priority range is from 1 - 255.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A regular expression consists of a character string presented in the form of a pattern, e.g., ‘^100 200$’. Refer to [ip bgp policy aspath-list](#) on page 30-136 for a table of valid regular expression characters (metacharacters). See also “Configuring BGP” in your Advanced Routing Guide for more information on using regular expressions in BGP commands.

- This command specifies the priority of an AS path list filter being applied to a peer’s inbound and outbound routes configured through the [ip bgp neighbor in-aspathlist](#), [ip bgp neighbor out-aspathlist](#), [ipv6 bgp neighbor in-aspathlist](#), and [ipv6 bgp neighbor out-aspathlist](#) commands. The AS path list filters routes based on one or more regular expressions, as shown in the example below. If the route matches the AS path list filter, then the permit or deny action (i.e., policy) associated with the regular expression applies, but only in the order designated by the priority value.

- The higher the priority value specified in the command, the later the matching is processed. For example, regular expressions with a priority of 1 (the default) are processed before an expression assigned a priority of 3. When regular expressions have an equal priority, the processing order is indeterminate.
• General or more specific AS path list information can be displayed by varying the use of the `show ip bgp policy aspath-list` command.

**Examples**

```
-> ip bgp policy aspath-list InboundAspath "^100 200$" priority 1
-> ip bgp policy aspath-list OutboundAspath "^300 400$" priority 5
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp neighbor in-aspathlist` Assigns an inbound AS path list filter to a BGP peer.
- `ip bgp neighbor out-aspathlist` Assigns an outbound AS path list filter to a BGP peer.
- `ip bgp policy aspath-list` Creates or removes an AS path list.
- `ip bgp policy aspath-list action` Configures a policy action (either permit or deny a route from passing) to be taken for an AS path list when a match is found.
- `ipv6 bgp neighbor in-aspathlist` Assigns an inbound AS path list filter to an IPv6 BGP peer.
- `ipv6 bgp neighbor out-aspathlist` Assigns an outbound AS path filter list to an IPv6 BGP peer.

**MIB Objects**

- `alaBgpAspathMatchListTable` Assigns an inbound AS path list filter to an IPv6 BGP peer.
- `alaBgpAspathMatchListPriority` Assigns an outbound AS path filter list to an IPv6 BGP peer.
**ip bgp policy community-list**

Creates or deletes a community list.

```
ip bgp policy community-list name {num:num | num.num:num | num}
no ip bgp policy community-list name {num:num | num.num:num | num}
```

### Syntax Definitions

- **name**
  Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.

- **num:num**
  The community number, given in the form of the AS number in the asplain format and the community number, separated by a colon.

- **num.num:num**
  The community number, given in the form of the AS number in the asdot or asdot+ format and the community number, separated by a colon.

### Defaults

No IP BGP peer policy community-list exists.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove a community-list.

- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.

- This command creates community lists that can be applied to a peer’s inbound and outbound routes using the `ip bgp neighbor in-communitylist`, `ip bgp neighbor out-communitylist`, `ipv6 bgp neighbor in-communitylist` and `ipv6 bgp neighbor out-communitylist` commands. The community list filters routes based on one or more community match list strings, as shown in the example below. If the route matches the community list filter, according to the matching type `exact` or `occur`, then the `permit` or `deny` policy action associated with the match list string applies.

- General or more specific community list information can be displayed by varying the use of the `show ip bgp policy community-list` command.

### Examples

```
-> ip bgp policy community-list CommListAIn 40:40
```
ip bgp policy community-list CommListAOut 400:20
no ip bgp policy community-list CommListAIn 40:40

Release History
Release 7.1.1; command was introduced.

Related Commands

- ip bgp neighbor inbound-community
  Assigns an inbound AS community list filter to a BGP peer.
- ip bgp neighbor outbound-community
  Assigns an outbound AS community list filter to a BGP peer.
- ip bgp policy community-list action
  Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
- ip bgp policy community-list match-type
  Configures type of matching to be performed with a community string list.
- ip bgp policy community-list priority
  Configures priority for processing multiple items in a community list filter.
- ipv6 bgp neighbor inbound-community
  Assigns an inbound community list filter to an IPv6 BGP peer.
- ipv6 bgp neighbor outbound-community
  Assigns an outbound community filter list to an IPv6 BGP peer.

MIB Objects
alaBgpCommunityMatchListTable
  alaBgpCommunityMatchListRowStatus
ip bgp policy community-list action

Configures the action to be taken for a community list when a match is found.

```
ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed | num:num} action {permit | deny}
```

### Syntax Definitions

- **name**: Community name, e.g., CommListAIIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
- **none**: Removes the community restrictions on the community section of the route map.
- **no-export**: Routes in this community are advertised within the AS but not beyond the local AS.
- **no-advertise**: Routes in this community are not advertised to any peer.
- **no-export-subconfed**: Routes in this community are not advertised to any external BGP peer.
- **num:num**: The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.
- **permit**: Allows matching routes to pass.
- **deny**: Stops matching routes from passing.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>permit</td>
</tr>
<tr>
<td>deny</td>
<td>deny</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- By default, this command allows routes that match the criteria specified in the community list to pass.
- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.

### Examples

```
-> ip bgp policy community-list commListAIIn 600:1 action permit
```
-> ip bgp policy community-list commListAIn 600:1 action deny

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to community string.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip bgp neighbor in-communitylist</td>
<td>Assigns an inbound AS community list filter to a BGP peer.</td>
</tr>
<tr>
<td>ip bgp neighbor out-communitylist</td>
<td>Assigns an outbound AS community list filter to a BGP peer.</td>
</tr>
<tr>
<td>ip bgp policy community-list match-type</td>
<td>Configures type of matching to be performed with a community string list.</td>
</tr>
<tr>
<td>ip bgp policy community-list priority</td>
<td>Configures priority for processing multiple items in a community list filter.</td>
</tr>
<tr>
<td>ipv6 bgp neighbor in-communitylist</td>
<td>Assigns an inbound community list filter to an IPv6 BGP peer.</td>
</tr>
<tr>
<td>ipv6 bgp neighbor out-communitylist</td>
<td>Assigns an outbound community filter list to an IPv6 BGP peer.</td>
</tr>
</tbody>
</table>

MIB Objects

alaBgpCommunityMatchListTable
  alaBgpCommunityMatchListAction
**ip bgp policy community-list match-type**

Configures the type of matching to be performed with a community string list.

```
ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed | num:num} match-type {exact | occur}
```

---

**Syntax Definitions**

- **name**: Community name, e.g., CommListAIn, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
- **none**: Removes the community restrictions on the community section of the route map.
- **no-export**: Routes in this community are advertised within the AS but not beyond the local AS.
- **no-advertise**: Routes in this community are not advertised to any peer.
- **no-export-subconfed**: Routes in this community are not advertised to any external BGP peer.
- **num:num**: The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
- **exact**: Checks for an exact match of the community string and the community attribute.
- **occur**: Checks for an occurrence of the community string anywhere in the community attribute.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>exact</td>
<td>occur</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, this command only allows routes to pass if the community string exactly matches the community attribute of the route.

**Examples**

```
-> ip bgp policy community-list commListC 600:1 match-type exact
```
**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to `community` string.

**Related Commands**

- `ip bgp neighbor in-communitylist` Assigns an inbound AS community list filter to a BGP peer.
- `ip bgp neighbor out-communitylist` Assigns an outbound AS community list filter to a BGP peer.
- `ip bgp policy community-list action` Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.
- `ip bgp policy community-list priority` Configures priority for processing multiple items in a community list filter.
- `ipv6 bgp neighbor in-communitylist` Assigns an inbound community list filter to an IPv6 BGP peer.
- `ipv6 bgp neighbor out-communitylist` Assigns an outbound community filter list to an IPv6 BGP peer.

**MIB Objects**

- `alaBgpCommunityMatchListTable`
  - `alaBgpCommunityMatchListType`
ip bgp policy community-list priority

Configures the priority for processing multiple items in a community list filter.

```
ip bgp policy community-list name {none | no-export | no-advertise | no-export-subconfed | num:num} priority value
```

**Syntax Definitions**

- **name**: Community name, e.g., CommListA1n, ranging from 0 to 70 characters, or a value of none. The Community name is case sensitive.
- **none**: Removes the community restrictions on the community section of the route map.
- **no-export**: Routes in this community are advertised within the AS but not beyond the local AS.
- **no-advertise**: Routes in this community are not advertised to any peer.
- **no-export-subconfed**: Routes in this community are not advertised to any external BGP peer.
- **num:num**: The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.
- **value**: Priority value in the range 0 - 255.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The higher the priority value specified in the command, the later the matching is processed. For example, items with a priority of 1 (the default) are processed before items assigned a priority of 3. When items have an equal priority, the processing order is indeterminate.

**Examples**

```
-> ip bgp policy community-list commListB 500:1 priority 3
```
Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to community string.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip bgp policy community-list</td>
<td>Creates or deletes a community list.</td>
</tr>
<tr>
<td>ip bgp policy community-list action</td>
<td>Configures a policy action (either permit or deny a route from passing) to be taken for an AS community list filter when a match is found.</td>
</tr>
<tr>
<td>ip bgp policy community-list match-type</td>
<td>Configures type of matching to be performed with community string list.</td>
</tr>
</tbody>
</table>

MIB Objects

alaBgpCommunityMatchListTable
alaBgpCommunityMatchListPriority
ip bgp policy prefix-list

Creates or deletes a prefix match list.

`ip bgp policy prefix-list name ip_address ip_mask`

`no ip bgp policy prefix-list name ip_address ip_mask`

**Syntax Definitions**

- `name`  Prefix list name.
- `ip_address`  IP address for the prefix list.
- `ip_mask`  Mask for the prefix list.

**Defaults**

No IP BGP policy prefix-list exists.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command creates prefix lists that can be applied to a peer’s inbound and outbound routes using the `ip bgp neighbor in-prefixlist`, `ip bgp neighbor out-prefixlist`, `ipv6 bgp neighbor in-prefixlist` and `ipv6 bgp neighbor out-prefixlist` commands. The prefix list filters routes based on one or more prefixes, as shown in the example below. If the route matches the prefix list filter, according to the `ge` (lower) and `le` (upper) limits defined, then the `permit` or `deny` action associated with the prefix applies.

- General or more specific prefix list information can be displayed by varying the use of the `show ip bgp policy prefix-list` command.

**Examples**

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip bgp neighbor in-prefixlist` Assigns an inbound prefix filter list to a BGP peer.
- `ip bgp neighbor out-prefixlist` Assigns an outbound prefix filter list to a BGP peer.
- `ip bgp policy prefix-list action` Configures action to be taken for a prefix list when a match is found.
- `ip bgp policy prefix-list ge` Configures lower limit on length of prefix to be matched.
- `ip bgp policy prefix-list le` Configures upper limit on length of prefix to be matched.
- `ipv6 bgp neighbor in-prefixlist` Assigns an inbound prefix filter list to an IPv6 BGP peer.
- `ipv6 bgp neighbor out-prefixlist` Assigns an outbound prefix filter list to an IPv6 BGP peer.

**MIB Objects**

- `alaBgpPrefixMatchListTable` 
- `alaBgpPrefixMatchListRowStatus`
**ip bgp policy prefix-list action**

Configures the action to be taken for a prefix list when a match is found.

```
ip bgp policy prefix-list name ip_address ip_mask action {permit | deny}
```

### Syntax Definitions

- `name` - Prefix list name.
- `ip_address` - IP address for the prefix list.
- `ip_mask` - Mask for the prefix list.
- `permit` - Allows matching routes to pass.
- `deny` - Stops matching routes from passing.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>permit</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/X48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 7.1.1</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Configures the action to be taken for a prefix list when a match is found.

### Examples

```
-> ip bgp policy prefix-list prefixListA 12.0.0.0 255.0.0.0 action deny
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ip bgp policy prefix-list` Creates or deletes a prefix match list.
- `ip bgp policy prefix-list ge` Configures lower limit on length of prefix to be matched.
- `ip bgp policy prefix-list le` Configures upper limit on length of prefix to be matched.

**MIB Objects**

- `alaBgpPrefixMatchListTable`
- `alaBgpPrefixMatchListAction`
ip bgp policy prefix-list ge

Configures the lower limit on the length of the prefix to be matched.

```
ip bgp policy prefix-list name ip_address ip_mask ge value
```

**Syntax Definitions**

- `name` Prefix list name.
- `ip_address` IP address for the prefix list.
- `ip_mask` Mask for the prefix list.
- `value` The lower limit value in the range 0 –32.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The default value of zero indicates there is no lower limit on the length of the prefix to be matched.
- This command is used in conjunction with the `ip bgp policy prefix-list le` command to set the prefix matching range. The two commands can be combined, as shown in the Example section below.
- The `ge` (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the `le` (upper limit) value.

**Examples**

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip bgp policy prefix-list` Creates or deletes a prefix match list.
- `ip bgp policy prefix-list action` Configures action to be taken for a prefix list when a match is found.
- `ip bgp policy prefix-list le` Configures upper limit on length of prefix to be matched.

**MIB Objects**

- `alaBgpPrefixMatchListTable`
- `alaBgpPrefixMatchListGE`
**ip bgp policy prefix-list le**

Configures the upper limit on the length of the prefix to be matched.

```
ip bgp policy prefix-list name ip_address ip_mask le value
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Prefix list name.</td>
</tr>
<tr>
<td>ip_address</td>
<td>Prefix list IP address for the prefix list.</td>
</tr>
<tr>
<td>ip_mask</td>
<td>Prefix list mask for the prefix list.</td>
</tr>
<tr>
<td>value</td>
<td>The upper limit value in the range of 0 to 32.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The default value of zero indicates there is no upper limit on the length of the prefix to be matched.
  This command is used in conjunction with `ip bgp policy prefix-list ge` to set the prefix matching range. The two commands can be combined, as show in the Example section below.
- The `ge` (lower limit) value must be greater than or equal to the prefix length (8 in the example below) and less than or equal to the `le` (upper limit) value.

### Examples

```
-> ip bgp policy prefix-list prefixListA 14.0.0.0 255.0.0.0 ge 8 le 16
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- `ip bgp policy prefix-list` Creates or deletes a prefix match list.
- `ip bgp policy prefix-list action` Configures action to be taken for a prefix list when a match is found.
- `ip bgp policy prefix-list ge` Configures lower limit on length of prefix to be matched.

MIB Objects

- `alaBgpPrefixMatchListTable`
- `alaBgpPrefixMatchListLE`
**ip bgp policy prefix6-list**

Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

```
ip bgp policy prefix6-list pfx_list_name prefix6/pfx_length [action {permit | deny}] [admin-state {enable | disable}] [ge [{mask_length}]] [le [{mask_length}]]
```

```
no ip bgp policy prefix6-list pfx_list_name prefix6/pfx_length [action {permit | deny}] [admin-state {enable | disable}] [ge [{mask_length}]] [le [{mask_length}]]
```

**Syntax Definitions**

- `pfx_list_name` Prefix list name.
- `prefix6` Prefix list IPv6 address for the prefix list.
- `pfx_length` Prefix length. Prefix length should be in the range of 0 to 128.
- `permit | deny` Action to be taken which can be either permit or deny.
- `enable | disable` Row Status can be either enabled or disabled.
- `mask_length` Minimum length of the prefix to be matched. The valid range is 0–32.

**Defaults**

NA

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable this feature.
- BGP must be configured on the system.
- This command creates prefix6 lists that can be applied to a peer's inbound and outbound routes using the `ip bgp neighbor in-prefix6list`, `ip bgp neighbor out-prefix6list`, `ipv6 bgp neighbor in-prefix6list` and `ipv6 bgp neighbor out-prefix6list`.
- The `ge` (lower limit) value must be greater than or equal to the prefix length and less than or equal to the `le` (upper limit) value.

**Examples**

- `-> ip bgp policy prefix6-list uniqLocal FC00::/48`
- `-> ip bgp policy prefix6-list uniqLocal FC00::/48 action permit`
- `-> ip bgp policy prefix6-list uniqLocal FC00::/48 admin-state enable`
-> no ip bgp policy prefix6-list uniqLocal FC00::/48

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip bgp policy prefix6-list` Displays prefix6 list parameters.
- `show ipv6 bgp neighbors` Displays the configured IPv6 BGP peers.
- `ip bgp neighbor in-prefix6list` Assigns an inbound prefix6 list to a BGP peer.
- `ip bgp neighbor out-prefix6list` Assigns an outbound prefix6 list to a BGP peer.
- `ipv6 bgp neighbor in-prefix6list` Assigns an inbound prefix6 list to an IPv6 BGP peer.
- `ipv6 bgp neighbor out-prefix6list` Assigns an outbound prefix6 list to an IPv6 BGP peer.

**MIB Objects**

- `alaBgpPrefix6MatchListTable`  
  - `alaBgpPrefix6MatchListId`  
  - `alaBgpPrefix6MatchListAddr`  
  - `alaBgpPrefix6MatchListAddrLength`  
  - `alaBgpPrefix6MatchListAction`  
  - `alaBgpPrefix6MatchListRowStatus`  
  - `alaBgpPrefix6MatchListGE`  
  - `alaBgpPrefix6MatchListLE`
**ip bgp policy route-map**

Creates or deletes a policy route map.

```
ip bgp policy route-map name sequence_number
```

**Syntax Definitions**

- **name**: Route map name. Case-sensitive.
- **sequence_number**: Route map sequence number in the range of 1 to 255. The sequence number allows for multiple instances of the same route map name.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command creates policy route maps. Each route map can be configured using the following match commands to specify the match criteria by which routes are allowed to pass. Match criteria is examined in the order the commands are listed below.
  1. `ip bgp policy route-map aspath-list`
  2. `ip bgp policy route-map prefix-list`
  3. `ip bgp policy route-map prefix6-list`
  4. `ip bgp policy route-map community-list`
  5. `ip bgp policy route-map match-regexp`
  6. `ip bgp policy route-map match-prefix`
  7. `ip bgp policy route-map match-mask`
  8. `ip bgp policy route-map match-prefix6`
  9. `ip bgp policy route-map match-community`

- The route maps which apply to a specific address family (IPv4 or IPv6) are only applied to routes of the same address family. In other words, the prefix-list filter and match-prefix/match-mask route-maps
are only applied to IPv4 routes and are ignored for IPv6 routes. The prefix6-list filter and match-

- Each route map can also be configured using the following set commands to sequentially specify the actions to be taken when a match is found.
  - ip bgp policy route-map community
  - ip bgp policy route-map community-mode
  - ip bgp policy route-map ipref
  - ip bgp policy route-map ipref-mode
  - ip bgp policy route-map med
  - ip bgp policy route-map med-mode
  - ip bgp policy route-map origin
  - ip bgp policy route-map weight

- Route maps can be referenced as a filtering mechanism for displaying paths using the show ip bgp path command. They are also referenced in filtering inbound and outbound routes for BGP peers using the ip bgp neighbor route-map commands.

Examples

-> ip bgp policy route-map routemap1 1

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy route-map action  Configures action to be taken for a route when a match is found.

MIB Objects

alaBgpRouteMapTable
  alaBgpRouteMapRowStatus
ip bgp policy route-map action

Configures the action to be taken for a route when a match is found.

```
ip bgp policy route-map name sequence_number action {permit | deny}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>A route map name.</td>
</tr>
<tr>
<td>sequence_number</td>
<td>A route map sequence number. The valid range is 1–255.</td>
</tr>
<tr>
<td>permit</td>
<td>Allows matching routes to pass.</td>
</tr>
<tr>
<td>deny</td>
<td>Stops matching routes from passing. In addition, no further instances</td>
</tr>
<tr>
<td></td>
<td>(sequence numbers) of the route map are examined.</td>
</tr>
</tbody>
</table>

**Defaultst**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>deny</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, this command allows routes that match the criteria specified in the route map to pass. If no matching routes are found, any additional instances (sequence numbers) of the route map name are examined. When all instances have been examined with no match, the route is dropped.

**Examples**

```
-> ip bgp policy route-map routemap1 1 action deny
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

```
ip bgp policy route-map
```

Creates or deletes a policy route map.

**MIB Objects**

```
alaBgpRouteMapTable
```

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 30-163
ip bgp policy route-map action

alaBgpRouteMapAction
ip bgp policy route-map aspath-list

Assigns an AS path matching list to the route map.

\textbf{ip bgp policy route-map name sequence_number aspath-list as_name}

### Syntax Definitions

- name: The route map name.
- sequence_number: The route map sequence number. The valid range is 1–255.
- as_name: The AS path list name or “none”.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>as_name</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- By default, no AS path list is assigned to a route map.
- This default behavior can be reset by changing the value of the AS path list name to “none”.
- The \textbf{ip bgp policy aspath-list} and \textbf{ip bgp policy aspath-list action} commands are used to create and set permit/deny actions for an AS path list.

### Examples

- -> ip bgp policy route-map routemap1 1 aspath-list aspathlist1
- -> ip bgp policy route-map routemap1 1 aspath-list none

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- \textbf{ip bgp policy route-map}: Creates or deletes a policy route map.

### MIB Objects

- \texttt{alaBgpRouteMapTable}
ip bgp policy route-map aspath-list

alaBgpRouteMapAsPathMatchListId
ip bgp policy route-map asprepend

Configures the AS path prepend action to be taken when a match is found.

```
ip bgp policy route-map name sequence_number asprepend path
```

Syntax Definitions

- `name` - The route map name.
- `sequence_number` - The route map sequence number. The valid range is 1–255.
- `path` - The AS path to prepend or “none”. Note that multiple AS path entries must be enclosed in quotes (e.g., “500 600 700”).

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>path</td>
<td>none</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

By default, no AS path is prepended. This command allows AS path numbers to be prepended (added to the beginning of the AS path list) to the AS path attribute of a matching route. The default behavior can be reset by changing the value to “none”.

Examples

```
-> ip bgp policy route-map routemap1 1 asprepend "700 800 900"
```

Release History

Release 7.1.1; command was introduced.
**Related Commands**

*ip bgp policy route-map*  
Creates or deletes a policy route map.

**MIB Objects**

alaBgpRouteMapTable

alaBgpRouteMapAsPrepend
ip bgp policy route-map community

Configures the action to be taken on the community attribute when a match is found.

```
ip bgp policy route-map name sequence_number community [none | no-export | no-advertise | no-export-subconfed | num:num]
```

**Syntax Definitions**

- **name**
  - The route map name.
- **sequence_number**
  - The route map sequence number. The valid range is 1–255.
- **none**
  - Removes the community restrictions on the community section of the route map.
- **no-export**
  - Routes in this community are advertised within the AS but not beyond the local AS.
- **no-advertise**
  - Routes in this community are not advertised to any peer.
- **no-export-subconfed**
  - Routes in this community are not advertised to any external BGP peer.
- **num:num**
  - The community number, given in the form of the AS number and the community number, separated by a colon (AS:NN), as defined in RFC 1997.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>no-export</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- By default, no action is taken on a community attribute when a match on a route is found.
- The default behavior can be reset by setting the value to “none”.
- The value of AS:NN is num.num:num if using asdot or asdot+ notation and is num:num if using asplain format.
The **ip bgp policy community-list** and **ip bgp policy community-list action** commands are used to create and set permit/deny actions for a community path list. This command is used in conjunction with **ip bgp policy route-map community-mode**.

**Examples**

```
-> ip bgp policy route-map routemap1 1 community 400:1 500:1
-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bgp policy route-map**
  - Creates or deletes a policy route map.

- **ip bgp policy route-map community-mode**
  - Configures the action to be taken for a community string when a match is found.

**MIB Objects**

- **alaBgpRouteMapTable**
  - **alaBgpRouteMapCommunity**
**ip bgp policy route-map community-list**

Assigns a community matching list to the route map.

```
ip bgp policy route-map name sequence_number community-list [list_name | none]
```

**Syntax Definitions**

- **name**
  - The route map name.
- **sequence_number**
  - The route map sequence number. The valid range is 1–255.
- **list_name**
  - The community list name.
- **none**
  - No community list name is specified.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_name</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, no community list is assigned to the route map. The default behavior can be reset by changing the value to `none`.

**Examples**

- `-> ip bgp policy route-map routemap1 1 community-list listB`
- `-> ip bgp policy route-map routemap1 1 community-list none`

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; syntax `none` added to `community-list` string.

**Related Commands**

- `ip bgp policy route-map` Creates or deletes a policy route map.

**MIB Objects**

alaBgpRouteMapTable
BGP Commands

ip bgp policy route-map community-list

alaBgpRouteMapCommunityMatchListId
**ip bgp policy route-map community-mode**

Configures the action to be taken for a community string when a match is found.

```
ip bgp policy route-map name sequence_number community-mode {add | replace}
```

### Syntax Definitions

- **name**
  - The route map name.

- **sequence_number**
  - The route map sequence number. The valid range is 1–255.

- **add**
  - Adds the community string specified in the command `ip bgp policy route-map community`

- **replace**
  - Replaces the community string specified in the command `ip bgp policy route-map community`

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>replace</td>
</tr>
<tr>
<td>add</td>
<td>replace</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is used in conjunction with `ip bgp policy route-map community`. The example on the next line shows the combined usage.

### Examples

- `-> ip bgp policy route-map routemap1 1 community-mode replace`
- `-> ip bgp policy route-map routemap1 1 community 400:1 500:1 community-mode replace`

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp policy route-map**
  Creates or deletes a policy route map.

- **ip bgp policy route-map community**
  Configures the action to be taken on the community attribute when a match is found.

MIB Objects

- **alaBgpRouteMapTable**
- **alaBgpRouteMapSetComunityMode**
ip bgp policy route-map lpref

Configures the local preference value for the route map.

ip bgp policy route-map name sequence_number lpref value

Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The route map name.</td>
</tr>
<tr>
<td>sequence_number</td>
<td>The route map sequence number. The valid range is 1–255.</td>
</tr>
<tr>
<td>value</td>
<td>The local preference value. The valid range is 0–4294967295.</td>
</tr>
</tbody>
</table>

Defaults

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is used in conjunction with ip bgp policy route-map lpref-mode. The example on the next line shows the combined usage.

- In this example, the local preference value will be incremented for a matching route by 555.

Examples

- ip bgp policy route-map routemap1 1 lpref 555
- ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc

Release History

Release 7.1.1; command was introduced.
Related Commands

- **ip bgp policy route-map**
  Creates or deletes a policy route map.

- **ip bgp policy route-map lpref-mode**
  Configures the action to be taken when setting local preference attribute for a local matching route.

MIB Objects

- alaBgpRouteMapTable
  - alaBgpRouteMapLocalPref
**ip bgp policy route-map lpref-mode**

Configures the action to be taken when setting local preference attribute for a local matching route.

```
ip bgp policy route-map name sequence_number lpref-mode {none | inc | dec | rep}
```

**Syntax Definitions**

- **name**: The route map name.
- **sequence_number**: The route map sequence number. The valid range is 1–255.
- **none**: Do not set the local preference attribute.
- **inc**: Increment the local preference attribute in the matching route by the value specified in the `ip bgp policy route-map med` command. No action is taken if no local preference attribute is found in the matching route.
- **dec**: Decrement the local preference attribute in the matching route by the value specified in the `ip bgp policy route-map med` command. No action is taken if no local preference attribute is found in the matching route.
- **rep**: Replace the local preference attribute in the matching route by the value specified in the `ip bgp policy route-map med` command even if no local preference attribute is found in the matching route.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>inc</td>
</tr>
<tr>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is used in conjunction with `ip bgp policy route-map lpref`. The example below shows the combined usage.
- In this example, the local preference value is incremented for a matching route by 555.

**Examples**

```
-> ip bgp policy route-map routemap1 l lpref-mode none
```
-> ip bgp policy route-map routemap1 1 lpref 555 lpref-mode inc

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp policy route-map` Creates or deletes a policy route map.
- `ip bgp policy route-map lpref` Configures the local preference value for the route map.
- `ip bgp policy route-map med` Configures the Multi-Exit Discriminator (MED) value for a route map.

**MIB Objects**

- `alaBgpRouteMapTable`
- `alaBgpRouteMapLocalPrefMode`
ip bgp policy route-map match-community

Configures a matching community primitive for the route map.

```
ip bgp policy route-map name sequence_number match-community [none | no-export | no-advertise | no-export-subconfed | num:num]
```

**Syntax Definitions**

- **name**: The route map name.
- **sequence_number**: The route map sequence number. The valid range is 1–255.
- **none**: Removes the community match from the route-map.
- **no-export**: Routes in this community are advertised within the AS but not beyond the local AS.
- **no-advertise**: Routes matching the community restricting advertisement to any peer.
- **no-export-subconfed**: Routes matching the community restricting advertisement to any external BGP peer.
- **num:num**: The community number, given in the form of the AS number and the community number, separated by a colon, as defined in RFC 1997.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>no-export</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command allows a matching community string primitive to be placed directly in the route map.
- By default, no community string is specified. The default behavior can be reset by changing the value to `none`.
- The value of AS:NN is `num:num:num` if using asdot or asdot+ notation and is `num:num` if using asplain format.
Examples

-> ip bgp policy route-map routemap1 1 match-community 400:1 500 700:1

Release History

Release 7.1.1; command was introduced.

Related Commands

`ip bgp policy route-map` Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable
   alaBgpRouteMapMatchCommunity
ip bgp policy route-map match-mask

Configures a matching mask primitive in the route map.

ip bgp policy route-map name sequence_number match-mask ip_address

**Syntax Definitions**

- **name**: The route map name.
- **sequence_number**: The route map sequence number. The valid range is 1–255.
- **ip_address**: The 32-bit IP address of the matching mask or “none”.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command allows a matching mask primitive to be placed directly in the route map. By default, no mask primitive is specified. The default behavior can be reset by changing the value to “none”.

- The example on the next line shows usage combined with the `ip bgp policy route-map match-prefix` command.

**Examples**

- `-> ip bgp policy route-map routemap1 1 match-mask 255.255.0.0`
- `-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `ip bgp policy route-map` creates or deletes a policy route map.
- `ip bgp policy route-map match-prefix` configures a matching prefix primitive in the route map.

MIB Objects

- `alaBgpRouteMapTable`  
  - `alaBgpRouteMapMatchMask`
ip bgp policy route-map match-prefix

Configures a matching prefix primitive in the route map.

\texttt{ip bgp policy route-map \textit{name} sequence\_number match\_prefix \textit{ip\_address}}

### Syntax Definitions

- **name**: The route map name.
- **sequence\_number**: The route map sequence number. The valid range is 1–255.
- **ip\_address**: The 32-bit IP address of the matching prefix.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command allows a matching prefix primitive to be placed directly in the route map. By default, no prefix primitive is specified. The default behavior can be reset by changing the value to “\texttt{none}”.

- The example on the next line shows usage combined with the \texttt{ip bgp policy route-map match-mask} command.

### Examples

- \texttt{-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0}
- \texttt{-> ip bgp policy route-map routemap1 1 match-prefix 17.0.0.0 match-mask 255.255.0.0}

### Release History

Release 7.1.1; command was introduced.
Related Commands

*ip bgp policy route-map match-mask*  Configures a matching prefix primitive in the route map.

*ip bgp policy route-map*  Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable

alaBgpRouteMapMatchPrefix
ip bgp policy route-map match-prefix6

Configures a matching prefix6 primitive in the route map.

**Syntax**

```
ip bgp policy route-map name sequence_number match-prefix6 ipv6_address/mask_length
```

**Syntax Definitions**

- `name`: The route map name.
- `sequence_number`: The route map sequence number. The valid range is 1–255.
- `ipv6_address/mask_length`: The 128-bit IPv6 address of the matching prefix. The length in bits of the IPv6 prefix to be matched in the Route Map.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command allows a matching prefix6 primitive to be placed directly in the route map. By default, no prefix6 primitive is assigned to the route map. The default behavior can be reset by changing the value to “none”.

**Examples**

- `-> ip bgp policy route-map routemap1 1 match-prefix6 2001:1218:103::/64`
- `-> ip bgp policy route-map routemap1 1 match-prefix6 none`

**Release History**

Release 7.3.4; command introduced.
**Related Commands**

ip bgp policy route-map

Creates or deletes a policy route map.

**MIB Objects**

alaBgpRouteMapTable

alaBgpRouteMapMatchPrefix6
alaBgpRouteMapMatchMaskLength6
ip bgp policy route-map match-regexp

Configures an AS path matching regular expression primitive in the route map.

```
ip bgp policy route-map name sequence_number match-regexp "regular_expression"
```

### Syntax Definitions

- **name**: The route map name.
- **sequence_number**: The route map sequence number. The valid range is 1–255.
- **regular_expression**: Regular expression or “none”. The regular expression must be enclosed by quotation marks.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>regular_expression</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command allows a regular expression matching directive to be placed directly in the route map. By default, no matching regular expression is specified. Regular expressions are defined in `ip bgp policy aspath-list` on page 30-136.
- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.
- The default behavior can be reset by changing the value to “none”.
- See the *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide* for more information on the use of regular expressions in BGP commands.

### Examples

```
-> ip bgp policy route-map routemap1 1 match-regexp "500 .* 400$"
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

ip bgp policy route-map

Creates or deletes a policy route map.

MIB Objects

alaBgpRouteMapTable
  alaBgpRouteMapMatchAsRegExp
**ip bgp policy route-map med**

Configures the Multi-Exit Discriminator (MED) value for a route map.

`ip bgp policy route-map name sequence_number med value`

---

**Syntax Definitions**

- `name` The route map name.
- `sequence_number` The route map sequence number. The valid range is 1–255.
- `value` The MED value. The valid range is 0–4294967295.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

This command is used in conjunction with `ip bgp policy route-map med-mode` command. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

**Examples**

- `-> ip bgp policy route-map routemap1 1 med 555`
- `-> ip bgp policy route-map routemap1 1 med 555 med-mode inc`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `ip bgp policy route-map med-mode` Configures Multi-Exit Discriminator (MED) value for a route map.
- `ip bgp policy route-map` Creates or deletes a policy route map.

MIB Objects

- `alaBgpRouteMapTable`
- `alaBgpRouteMapMed`
ip bgp policy route-map med-mode

Configures the action to be taken when setting the Multi-Exit Discriminator (MED) attribute for a matching route.

\[ \text{ip bgp policy route-map name sequence_number med-mode \{none | inc | dec | rep\}} \]

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The route map name.</td>
</tr>
<tr>
<td>sequence_number</td>
<td>The route map sequence number. The valid range is 1–255.</td>
</tr>
<tr>
<td>value</td>
<td>The MED value. The valid range is 0–4294967295.</td>
</tr>
<tr>
<td>none</td>
<td>Do not set the MED.</td>
</tr>
<tr>
<td>inc</td>
<td>Increment the MED in the matching route by the value specified in the ip bgp policy route-map med command. No action is taken if no MED is found in the matching route.</td>
</tr>
<tr>
<td>dec</td>
<td>Decrement the MED in the matching route by the value specified in the ip bgp policy route-map med command. No action is taken if no MED is found in the matching route.</td>
</tr>
<tr>
<td>rep</td>
<td>Replace the MED in the matching route by the value specified in the ip bgp policy route-map med command even if no MED is found in the matching route.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>inc</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is used in conjunction with ip bgp policy route-map med. The first example below shows the combined usage. In the second example, the MED value is incremented for a matching route by 5.

### Examples

- -> ip bgp policy route-map routemap1 1 med-mode inc
- -> ip bgp policy route-map routemap1 1 med 5 med-mode inc
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp policy route-map med` Configures action to take when setting Multi-Exit Discriminator (MED) attribute for a matching route.
- `ip bgp policy route-map` Creates or deletes a policy route map.

**MIB Objects**

- `alaBgpRouteMapTable`
- `alaBgpRouteMapMedMode`
ip bgp policy route-map origin

Configures the action to be taken on the origin attribute when a match is found.

`ip bgp policy route-map name sequence_number origin {igp | egp| incomplete | none}`

**Syntax Definitions**

| name | The route map name. |
| sequence_number | The route map sequence number. The valid range is 1–255. |
| igp | Sets the origin attribute to remote internal BGP (IGP). |
| egp | Sets the origin attribute to local external BGP (EGP). |
| incomplete | Sets the origin attribute to incomplete, meaning the origin is unknown. |
| none | Sets the origin attribute to “none”. |

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>igp</td>
<td>none</td>
</tr>
<tr>
<td>egp</td>
<td>none</td>
</tr>
<tr>
<td>incomplete</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, no action is taken on the origin attribute when a match is found. The default behavior can be reset by changing the value to “none”.

**Examples**

`-> ip bgp policy route-map routemap1 1 origin egp`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip bgp policy route-map origin` Configures action to take on origin attribute when a match is found.
- `ip bgp policy route-map` Creates or deletes a policy route map.

**MIB Objects**

- `alaBgpRouteMapTable`
- `alaBgpRouteMapOrigin`
ip bgp policy route-map prefix-list

Assigns a prefix matching list to the route map.

`ip bgp policy route-map name sequence_number prefix-list prefix_name`

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The route map name.</td>
</tr>
<tr>
<td>sequence_number</td>
<td>The route map sequence number. The valid range is 1–255.</td>
</tr>
<tr>
<td>prefix_name</td>
<td>The prefix list name or “none”.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix_name</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- By default, no prefix list is assigned to the route map. The default behavior can be reset by changing the value to “none”.
- The `ip bgp policy prefix-list`, `ip bgp policy prefix-list action`, `ip bgp policy prefix-list ge`, and `ip bgp policy prefix-list le` commands are used to create and set permit/deny actions for a prefix path list.

### Examples

```
-> ip bgp policy route-map routemap1 1 prefix-list listC
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- `ip bgp policy prefix-list` Assigns a prefix matching list to the route map.
- `ip bgp policy prefix-list action` Configures the action taken for a prefix list when a match is found.
- `ip bgp policy route-map` Creates or deletes a policy route map.

MIB Objects

- `alaBgpRouteMapTable`
  - `alaBgpRouteMapPrefixMatchListId`
**ip bgp policy route-map prefix6-list**

Assigns a prefix6 matching list to the route map, which identifies the matching criteria list of IPv6 prefixes.

```
ip bgp policy route-map name sequence_number prefix6-list prefix6_name
```

---

**Syntax Definitions**

- **name**: The route map name.
- **sequence_number**: The route map sequence number. The valid range is 1–255.
- **prefix6_name**: The prefix6 list name or “none”.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix6_name</td>
<td>none</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The prefix6-list policy name is created using the `ip bgp policy prefix6-list` command.
- By default, no prefix6 list is assigned to the route map. The default behavior can be reset by changing the value to “none”.

---

**Examples**

```
-> ip bgp policy route-map routemap1 1 prefix6-list listB
-> ip bgp policy route-map routemap1 1 prefix6-list none
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `ip bgp policy prefix6-list`: Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

---

**MIB Objects**

- `alaBgpRouteMapTable`
ip bgp policy route-map prefix6-list

alaBgpRouteMapPrefix6MatchListId
**ip bgp policy route-map weight**

Configures a BGP weight value to be assigned to inbound routes when a match is found.

**Syntax**

```
ip bgp policy route-map name sequence_number weight value
```

**Syntax Definitions**

- `name`: The route map name.
- `sequence_number`: The route map sequence number. The valid range is 1–255.
- `value`: The weight value. The valid range is 0–65535.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command sets the weight value for routes that pass the route map match criteria. It is only applicable for the inbound policy. The default value of zero means that the weight is not changed by the route map.

**Examples**

```
-> ip bgp policy route-map routemap1 1 weight 500
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bgp policy route-map**: Creates or deletes a policy route map.

**MIB Objects**

- `alaBgpRouteMapTable`
- `alaBgpRouteMapWeight`
**ip bgp policy route-map community-strip**

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

```
ip bgp policy route-map name sequence_number community-strip community_list
```

**Syntax Definitions**

- `name`: The route map name.
- `sequence_number`: The route map sequence number. The valid range is 1–255.
- `community_list`: The community list name.

**Defaults**

No IP BGP policy route-map community list exists.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported/Enabled</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configures the value to strip from the community attribute of the routes matched by this route map instance (sequence number).

**Examples**

```
-> ip bgp policy route-map routemap1 1 community_strip communitylist
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp policy route-map`: Creates or deletes a policy route map.

**MIB Objects**

- `alaBgpRouteMapTable`
- `alaBgpRouteMapCommunityStrip`
**show ip bgp**

Displays the current global settings for the local BGP speaker.

**show ip bgp**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Most of the parameters in this display can be altered through BGP global commands. See the output definitions below for references to the CLI commands used to configure individual parameters.

**Examples**

-> show ip bgp
Admin Status = disabled,
Operational Status = up,
Autonomous system Number = 1,
BGP Router Id = 111.1.1.1,
Confederation Identifier = 0,
IGP Synchronization Status = disabled,
Minimum AS origin interval (seconds) = 15,
Default Local Preference = 100,
Route Reflection = disabled,
Cluster Id = 0.0.0.0,
Missing MED Status = Best,
Aspath Comparison = enabled,
Always Compare MED = disabled,
Fast External Fail Over = disabled,
Log Neighbor Changes = disabled,
Multiple path = enabled,
Graceful Restart = enabled,
Graceful Restart Status = Not Restarting,
Configured Graceful Restart Interval = 90s,
IPv4 Unicast = enabled,
IPv6 Unicast = disabled,
<table>
<thead>
<tr>
<th>Command</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Status</td>
<td>disabled</td>
</tr>
<tr>
<td>ASN Output Format</td>
<td>asplain</td>
</tr>
<tr>
<td><strong>output definitions</strong></td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Admin Status</strong></td>
<td>Indicates whether the BGP protocol has been enabled or disabled through the <code>ip bgp admin-state</code> command.</td>
</tr>
<tr>
<td><strong>Operational Status</strong></td>
<td>Indicates if the local BGP speaker is actively participating in BGP messages, update, routing advertisements.</td>
</tr>
<tr>
<td><strong>Autonomous system Number</strong></td>
<td>The AS assigned to the local BGP speaker through the <code>ip bgp autonomous-system</code> command.</td>
</tr>
<tr>
<td><strong>BGP Router Id</strong></td>
<td>The IP address for the local BGP speaker.</td>
</tr>
<tr>
<td><strong>Confederation Id</strong></td>
<td>Shows the confederation number assigned to the local BGP speaker. If the BGP speaker does not belong to a confederation, then this value will be zero (0). Confederation numbers are assigned through the <code>ip bgp confederation identifier</code> command.</td>
</tr>
<tr>
<td><strong>IGP Synchronization Status</strong></td>
<td>Indicates whether BGP is synchronizing its routing tables with those on non-BGP routers handling IGP traffic (such as a RIP or OSPF router). Configured through the <code>ip bgp synchronization</code> command.</td>
</tr>
<tr>
<td><strong>Minimum AS origin interval</strong></td>
<td>The frequency, in seconds, at which routes local to the autonomous system are advertised. Configured through the <code>ip bgp as-origin-interval</code> command.</td>
</tr>
<tr>
<td><strong>Default Local Preference</strong></td>
<td>The local preference that will be assigned to routes that do not already contain a local preference value. This default value is configured through the <code>ip bgp default local-preference</code> command.</td>
</tr>
<tr>
<td><strong>Route Reflection</strong></td>
<td>Indicates whether the local BGP speaker is acting as a route reflector for its AS. Configured through the <code>ip bgp client-to-client reflection</code> command.</td>
</tr>
<tr>
<td><strong>Cluster Id</strong></td>
<td>The IP address for cluster in route reflector configurations using multiple, redundant route reflectors. A value of 0.0.0.0 indicates that a cluster is not set up. Configured through the <code>ip bgp cluster-id</code> command.</td>
</tr>
<tr>
<td><strong>Missing MED Status</strong></td>
<td>Indicates the MED value that will be assigned to paths that do not contain MED values. Missing MED values will either be assigned to the worst possible value (2^{32}-1) or the best possible value (0). This value is set using the <code>ip bgp bestpath med missing-as-worst</code> command. By default, missing MED values are treated as best.</td>
</tr>
<tr>
<td><strong>Aspath Comparison</strong></td>
<td>Indicates whether the AS path will be in used in determining the best route. Configured through the <code>ip bgp bestpath as-path ignore</code> command.</td>
</tr>
<tr>
<td><strong>Always Compare MED</strong></td>
<td>Indicates whether multi-exit discriminator (MED) values are being compared only for internal peers or also for external peers. Configured through the <code>ip bgp always-compare-med</code> command.</td>
</tr>
<tr>
<td><strong>Fast External Fail Over</strong></td>
<td>Indicates whether Fast External Failover has been enabled or disabled. When enabled a BGP sessions will be reset immediately after a connection to a directly connected external peer goes down. Configured through the <code>ip bgp fast-external-failover</code> command.</td>
</tr>
<tr>
<td><strong>Log Neighbor Changes</strong></td>
<td>Indicates whether logging of peer state changes is enabled or disabled. Configured through the <code>ip bgp log-neighbor-changes</code> command.</td>
</tr>
<tr>
<td><strong>Multi path</strong></td>
<td>Indicates whether support for multiple equal cost paths is enabled or disabled. Configured through the <code>ip bgp maximum-paths</code> command.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful Restart</td>
<td>Indicates whether graceful restart is enabled or disabled.</td>
</tr>
<tr>
<td>Graceful Restart Status</td>
<td>Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.</td>
</tr>
<tr>
<td>Configured Graceful Restart Interval</td>
<td>Indicates the timer for achieving a graceful restart.</td>
</tr>
<tr>
<td>IPv4 Unicast</td>
<td>Indicates whether IPv4 unicast is enabled or disabled.</td>
</tr>
<tr>
<td>IPv6 Unicast</td>
<td>Indicates whether IPv6 unicast is enabled or disabled.</td>
</tr>
<tr>
<td>BFD Status</td>
<td>Indicates whether BFD is enabled or disabled for the BGP protocol. Configured through the bgp neighbor check-first-as command.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

- `ip bgp unicast` Enables or disables unicast IPv4 updates for the BGP routing process.
- `ipv6 bgp unicast` Enables or disables unicast IPv6 updates for the BGP routing process.
- `show ip bgp statistics` Displays BGP global statistics.

MIB Objects

```
alabgpMIBGlobalsGroup
  alaBgpProtoStatus
  alaBgpAutonomousSystemNumber
  alaBgpIgpSynchStatus
  alaBgpProtoOperState
  alaBgpNumActiveRoutes
  alaBgpNumEstabExternalPeers
  alaBgpNumEstabInternalPeers
  alaBgpClusterId
  alaBgpDefaultLocalPref
  alaBgpFastExternalFailOver
  alaBgpMedAlways
  alaBgpMissingMed
  alaBgpRouterId
  alaBgpRouteReflection
  alaBgpAsOriginInterval
  alaNumIgpSynchWaitPaths
  alaBgpManualTag
  alaBgpPromiscuousneighbors
  alaBgpConfedId
  alaBgpMultiPath
  alaBgpMaxPeers
  alaBgpPeersChanges
```
**show ip bgp statistics**

Displays BGP global statistics.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command show various BGP statistics for the router, such as number of neighbors, active prefixes, number of paths, etc.

**Examples**

```bash
-> show ip bgp statistics
# of Active Prefixes Known = 0,
# of EBGP Neighbors in Established State = 0,
# of IBGP Neighbors in Established State = 0,
# of Feasible Paths = 0,
# of Dampened Paths = 0,
# of Unsynchronized Paths = 0,
# of Policy unfeasible paths = 0,
Total Number of Paths = 0
```

**output definitions**

<table>
<thead>
<tr>
<th># of Active Prefixes Known</th>
<th>The number of prefixes, or route paths, currently known to the local BGP speaker, that are currently up and active.</th>
</tr>
</thead>
<tbody>
<tr>
<td># of EBGP Neighbors in Established State</td>
<td>The number of peers outside the AS of the local BGP speaker that the local BGP speaker can route to.</td>
</tr>
<tr>
<td># of IBGP Neighbors in Established State</td>
<td>The number of peers in the same AS as the local BGP speaker that the local BGP speaker can route to.</td>
</tr>
<tr>
<td><strong>output definitions (continued)</strong></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td># of Feasible Paths</td>
<td>The number of route paths that are not active due to one of the following reasons: the route is dampened, the route is not permitted based on BGP policies, or the route is waiting to be synchronized with the IGP protocol.</td>
</tr>
<tr>
<td># of Dampered Paths</td>
<td>The number of route paths that are not active because they have violated dampening parameters.</td>
</tr>
<tr>
<td># of Unsynchronized Paths</td>
<td>The number of route paths that are not active because they are waiting to be synchronized with the IGP routing protocol.</td>
</tr>
<tr>
<td># of Unfeasible Paths</td>
<td>The number of route paths that are not active because they are not permitted based on a configured BGP policy.</td>
</tr>
<tr>
<td>Total Number of Paths</td>
<td>The total number of paths known to the speaker, active or not.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

*show ip bgp* Displays the current global settings for the local BGP speaker.

**MIB Objects**

*alaBgpStatsTable*
show ip bgp dampening

Displays the BGP route dampening settings.

show ip bgp dampening

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command shows the setting for dampening on the router, assuming it is enabled.

Examples

```bash
-> show ip bgp dampening
Admin Status                   = disabled,
Half life value (seconds)      = 300,
Reuse value                    = 200
Suppress value                 = 300,
Max suppress time (seconds)    = 1800,
```

Output definitions

- **Admin Status**
  Indicates whether route dampening is enabled or disabled. This value is configured through the `ip bgp dampening` command.

- **Half life value**
  The half-life interval, in seconds, after which the penalty value for a reachable route will be reduced by half. This value is configured through the `ip bgp dampening` command.

- **Reuse value**
  The value that the route flapping metric must reach before this route is re-advertised. This value is configured through the `ip bgp dampening` command.
**output definitions (continued)**

<table>
<thead>
<tr>
<th><strong>Suppress value</strong></th>
<th>The number of route withdrawals necessary to begin readvertising a previously suppressed route. This value is configured through the <code>ip bgp dampening</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max Suppress time</strong></td>
<td>The maximum time (in seconds) that a route will be suppressed. This value is configured through the <code>ip bgp dampening</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`ip bgp dampening` Enables or disables BGP route dampening or the suppression of unstable routes.

**MIB Objects**

alaBgpDampTable

- alaBgpDampEntry
- alaBgpDampCeil
- alaBgpDampCutOff
- alaBgpDampMaxFlapHistory
- alaBgpDampReuse
- alaBgpDampening
- alaBgpDampeningClear
show ip bgp dampening-stats

Displays BGP dampening statistics.

**show ip bgp dampening-stats [ip_address ip_mask] [peer_address]**

### Syntax Definitions

- **ip_address**: A 32-bit IP address.
- **ip_mask**: A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.
- **peer_address**: A 32-bit IP address of peer (neighbor).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays various statistics on routes that have flapped, and are thus subject to the settings of the dampening feature.

### Examples

```
-> show ip bgp dampening-stats
Network Mask From Flaps Duration FOM
----------------- ------------------ ------------- ----------------- -------
155.132.44.73 255.255.255.255 192.40.4.121 8 00h:00m:35s 175
```

### output definitions

- **Network**: The IP address for the local BGP speaker that is responsible for route dampening in this router.
- **Mask**: The mask for the local BGP speaker that is responsible for route dampening in this router.
- **From**: The IP address for the route that is flapping.
output definitions (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flaps</td>
<td>The number of times this route has moved from an UP state to a DOWN state or from a DOWN state to an UP state. If the route goes down and then comes back up, then this statistics would count 2 flaps.</td>
</tr>
<tr>
<td>Duration</td>
<td>The time since the first route flap occurred. In the above example, this route has flapped 8 times in a 35 second period.</td>
</tr>
<tr>
<td>FOM</td>
<td>The Figure Of Merit, or instability metric, for this route. This value increases with each unreachable event. If it reaches the cutoff value (configured in ip bgp dampening), then this route will no longer be advertised.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

**ip bgp dampening** Enables and disables route dampening.

MIB Objects

N/A
**show ip bgp path**

Displays BGP paths.

```
show ip bgp path
[ip-addr ip_address ip_mask]
[aspath-list aspathlist_name]
[community-list community_list_name]
[prefix-list prefix_name]
[route-map routemap_name]
[cidr-only]
[community community_number]
[neighbor-rcv recv_peer_address]
[neighbor-adv adv_peer_addr]
-regexp "regular_expression"
[best]
[detail]
```

### Syntax Definitions

- **ip_address**: A 32-bit IP address of the path.
- **ip_mask**: A 32-bit subnet mask of the path.
- **aspathlist_name**: AS path on which to filter.
- **community_list_name**: Community name on which to filter.
- **prefix_name**: Prefix on which to filter.
- **routemap_name**: Route map on which to filter.
- **clidr-only**: Filter out everything except CIDR routes.
- **community_number**: Community number on which to filter.
- **recv_peer_address**: Filter all except paths received from this path.
- **adv_peer_addr**: Filter all except paths sent to this path.
- **regular_expression**: Regular expression on which to filter. Regular expressions must be enclosed by quotes. For example, “$100”.
- **best**: Show only the best path.

### Defaults

N/A
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The basic command displays every path currently in the table. Since the number of paths may run into the thousands, this command provides a number of parameters for displaying a specific path or matching entries for a portion of a path or peer address.

- ‘Detail’ option displays the AS Path details for a specific route.

Examples

```
-> show ip bgp path
Legends: Sta = Path state
> = best, F = feasible
P = policy changing, U = un-synchronized
D = dampened, N = none
Nbr = Neighbor
(O) = Path Origin (? = incomplete, i = igp, e = egp)
degPref = degree of preference

<table>
<thead>
<tr>
<th>Sta</th>
<th>Network</th>
<th>Mask</th>
<th>Nbr address</th>
<th>Next Hop</th>
<th>(O)</th>
<th>degPref</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>192.40.4.0</td>
<td>255.255.255.0</td>
<td>192.40.4.29</td>
<td>192.40.4.29</td>
<td>i</td>
<td>100</td>
</tr>
<tr>
<td>&gt;</td>
<td>192.40.6.0</td>
<td>255.255.255.248</td>
<td>192.40.4.29</td>
<td>192.40.4.29</td>
<td>i</td>
<td>100</td>
</tr>
<tr>
<td>&gt;</td>
<td>192.40.6.8</td>
<td>255.255.255.248</td>
<td>192.40.4.29</td>
<td>192.40.4.29</td>
<td>i</td>
<td>100</td>
</tr>
</tbody>
</table>
```

```
U 110.100.10.0 255.255.255.0 2001:100:3::1 110.100.10.20 ? 100
U 110.100.11.0 255.255.255.0 2001:100:3::1 110.100.10.20 ? 100
U 110.100.12.0 255.255.255.0 2001:100:3::1 110.100.10.20 ? 100
U 110.100.13.0 255.255.255.0 2001:100:3::1 110.100.10.20 ? 100
U 110.100.14.0 255.255.255.0 2001:100:3::1 110.100.10.20 ? 100

-> show ip bgp path detail
Legends: Sta = Path state
> = best, F = feasible, S = stale
P = policy changing, U = un-synchronized
D = dampened, N = none
Nbr = Neighbor
(O) = Path Origin (? = incomplete, i = igp, e = egp)
degPref = degree of preference

<table>
<thead>
<tr>
<th>Sta</th>
<th>Network</th>
<th>Nbr address</th>
<th>Next Hop</th>
<th>degPref AS Path, (O)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>192.168.1.0/32</td>
<td>20.20.20.2</td>
<td>20.20.20.2</td>
<td>100 65535 65530, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>192.168.2.0/32</td>
<td>20.20.20.2</td>
<td>20.20.20.2</td>
<td>100 65535 65530, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>192.168.3.0/32</td>
<td>20.20.20.2</td>
<td>20.20.20.2</td>
<td>100 65535 65530, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>197.169.1.0/32</td>
<td>21.20.20.2</td>
<td>21.20.20.2</td>
<td>140 65536, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>197.169.2.0/32</td>
<td>21.20.20.2</td>
<td>21.20.20.2</td>
<td>140 65536, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>197.169.3.0/32</td>
<td>21.20.20.2</td>
<td>21.20.20.2</td>
<td>140 65536, i</td>
</tr>
</tbody>
</table>
```
-> show ip bgp path ip-addr 192.40.6.72 255.255.255.248
BGP Path parameters
Path address = 192.40.6.72
Path mask = 255.255.255.248
Path protocol = ebgp
Path peer = 192.40.4.29
  Path nextHop = 192.40.4.29,
  Path origin = igp,
  Path local preference = -1,
  Path state = active,
  Path weight = 0,
  Path preference degree = 100,
  Path autonomous systems = [nAs=2] : 3 2 ,
  Path MED = -1,
  Path atomic = no,
  Path AS aggregator = <none>,
  Path IPaddr aggregator = <none>,
  Path community = <none>,
  Path unknown attribute = <none>

output definitions

| Sta | Status flag. A greater-than sign (>) indicates this is the best route to the destination. |
| Network | The IP address for this route path. This is the destination of the route. |
| Mask | The mask for this route path. |
| Nbr address | The IP or IPv6 address of the BGP peer that is advertising this path. |
| Next Hop | The next hop along the route path. |
| (0) | The origin attribute of this route path. A question mark (?) indicates incomplete, and i indicates IGP, and an e indicates EGP. |
| degPref | The local preference value assigned to this route path. |

output definitions

| Path address | The IP address for route path. |
| Path mask | The mask for this route path. |
| Path protocol | The protocol from which this route path was learned. Possible values for this field are as follows: local, static, directhost, rip, ospf, isis, ibgp, ebgp, and other. |
| Path peer | The IP address of the peer that is advertising this route path. |
| Path nextHop | The next hop along the route path. |
| Path origin | The BGP origin attribute. Possible values will be igp, egp, incomplete, and none. The origin attribute is considered during the route decision process. |
| Path local preference | The local preference value for this route as received in an UPDATE message. A negative value (for example, the -1 in the above display) indicates that the local preference value is missing for this route path. |
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path state</td>
<td>Path state indicates the state of the path. The possible states are <strong>best</strong>, <strong>feasible</strong>, <strong>policy-wait</strong>, <strong>un-synchronized</strong>, <strong>dampened</strong>, or <strong>none</strong>. When path state is <strong>none</strong>, it indicates that there are no paths to this prefix and the route is being purged from the system.</td>
</tr>
<tr>
<td>Path weight</td>
<td>The path weight as assigned through inbound and outbound policies.</td>
</tr>
<tr>
<td>Path preference degree</td>
<td>The local preference assigned to this route through an inbound or outbound policy, or, if the local preference value is missing, the default local preference (which is assigned through the <code>ip bgp default local-preference</code>).</td>
</tr>
<tr>
<td>Path autonomous systems</td>
<td>The AS path for this route. These numbers show the ASs through which the route has traversed with the most recent AS listed first. In the above example, this route began its path in AS 2 and then traveled through AS 3.</td>
</tr>
<tr>
<td>Path MED</td>
<td>The multi-exit discriminator (MED) value for this route path. A negative value (for example, the <code>-1</code> in the above display) indicates that the MED value is missing for this route path.</td>
</tr>
<tr>
<td>Path atomic</td>
<td>Indicates whether the ATOMIC-AGGREGATE attribute has been set for this route. When set (this field would read <strong>yes</strong>), this attribute indicates that an aggregate has caused a loss of information for this route (a less specific route was chosen over a more specific route included in the aggregate).</td>
</tr>
<tr>
<td>Path AS aggregator</td>
<td>Part of the AGGREGATOR attribute. This field indicates the AS for the BGP speaker that created the aggregate. A value of <code>&lt;none&gt;</code> indicates this is not an aggregate route.</td>
</tr>
<tr>
<td>Path IPaddr aggregator</td>
<td>Part of the AGGREGATOR attribute. This field indicates the IP address for the BGP speaker that created the aggregate. A value of <code>&lt;none&gt;</code> indicates that this is not an aggregate route.</td>
</tr>
<tr>
<td>Path community</td>
<td>Indicates the community to which this route path belongs, if applicable. A value of <code>&lt;none&gt;</code> indicates that this route does not belong to a community.</td>
</tr>
<tr>
<td>Path unknown attribute</td>
<td>Indicates BGP attributes found in UPDATE messages which the router does not support. For example, multi-protocol attributes are not supported by the router in this release, but it is possible for these attributes to appear in a BGP route.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; **detail** keyword added.

**Related Commands**

- `show ip bgp routes` Displays BGP route details.

**MIB Objects**

- `alaBgpPathTable`
- `alaBgpPathEntry`
### show ip bgp routes

Displays BGP route details.

**Syntax**

```
show ip bgp routes [ip_address ip_mask]
```

### Syntax Definitions

- **ip_address**
  - A 32-bit IP address.

- **ip_mask**
  - A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays all the routes in the routing table with details.

### Examples

```
-> show ip bgp routes
```

Legends: ECL = EBGP change list, ICC = IBGP client change list
  ICL = IBGP change list, LCL = local change list
  AGG = Aggregation, AGC = Aggregation contribution
  AGL = Aggregation list, GDL = Deletion list
  AGW = Aggregation waiting, AGH = Aggregation hidden
  DMP = Dampening, ACT = Active route

<table>
<thead>
<tr>
<th>Address</th>
<th>Mask</th>
<th>ECL</th>
<th>ICC</th>
<th>ICL</th>
<th>LCL</th>
<th>AGG</th>
<th>AGC</th>
<th>AGL</th>
<th>AGW</th>
<th>AGH</th>
<th>GDL</th>
<th>DMP</th>
<th>ACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.40.4.0</td>
<td>255.255.255.0</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>192.40.6.0</td>
<td>255.255.255.248</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>192.40.6.8</td>
<td>255.255.255.248</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>192.40.6.72</td>
<td>255.255.255.248</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>192.40.6.80</td>
<td>255.255.255.248</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>192.40.6.104</td>
<td>255.255.255.248</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>192.40.6.112</td>
<td>255.255.255.248</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
output definitions

Address: The route destination network address.
Mask: The route destination network mask.
ECL: External BGP change list. When Yes, this route will be advertised as soon as the route advertisement timer expires.
ICC: Internal BGP client change list. When Yes, this route will be advertised to internal non-clients.
ICL: Internal BGP change list. When Yes, this route has changes that need to be advertised.
LCL: Local change list. When Yes, this route is local.
AGG: Aggregation. When Yes, this route is an aggregate route.
AGC: Aggregation contribution. When Yes, this route is part of an aggregate route.
AGL: Aggregation list. When Yes, this route is placed on an aggregate list.
AGW: Aggregation waiting. When Yes, this route is waiting for an aggregate contributor.
AGH: Aggregation hidden. When Yes, this route is hidden as part of an aggregate route.
GDL: Deletion list. When Yes, this route will be deleted.
DMP: Dampening. Indicate whether this route has been dampened. If ‘Yes’, then this route has been dampened and a dampening history exists.
ACT: Active route. When Yes, the route is active.

Release History

Release 7.1.1; command was introduced.

Related Commands

**show ip bgp path** Displays BGP paths.

MIB Objects

alaBgpRouteTable
alaBgpRouteEntry
**show ip bgp aggregate-address**

Displays aggregate route status.

```
show ip bgp aggregate-address [ip_address ip_mask]
```

### Syntax Definitions

- **ip_address**: A 32-bit IP address of the aggregate address.
- **ip_mask**: A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays a specific aggregate address, or all aggregate addresses on the router.

### Examples

```
-> show ip bgp aggregate-address
Network         Mask            Summarize As-Set   Admin state Oper state
---------------+---------------+---------+--------+-----------+----------
155.132.44.73   255.255.255.255 disabled  disabled disabled    not_active
192.40.6.0      255.255.255.255 disabled  disabled disabled    not_active

-> show ip bgp aggregate-address 192.40.6.0 255.255.255.255
Aggregate address  = 192.40.6.0,
Aggregate mask     = 255.255.255.255,
Aggregate admin state = disabled,
Aggregate oper state = not_active,
Aggregate as-set = disabled,
Aggregate summarize = disabled,
Aggregate metric = 0,
Aggregate local preference = 0,
Aggregate community string = 0:500 400:1 300:2
```
**Output Definitions**

<table>
<thead>
<tr>
<th>Network or Aggregate Address</th>
<th>The IP address for this aggregate route. This value is configured through the <code>ip bgp aggregate-address</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mask or Aggregate Mask</td>
<td>The mask for this aggregate route. This value is configured through the <code>ip bgp aggregate-address</code> command.</td>
</tr>
<tr>
<td>Summarize or Aggregate Summarize</td>
<td>Indicates whether aggregate summarization is enabled or disabled for this aggregate route. This value is configured through the <code>ip bgp aggregate-address summary-only</code> command.</td>
</tr>
<tr>
<td>As-Set or Aggregate as-set</td>
<td>Indicates whether AS path aggregate is enabled or disabled. This value is configured through the <code>ip bgp aggregate-address as-set</code> command.</td>
</tr>
<tr>
<td>Admin State or Aggregate Admin State</td>
<td>Indicates whether this aggregate route is administratively enabled or disabled. This value is configured through the <code>ip bgp aggregate-address admin-state</code> command.</td>
</tr>
<tr>
<td>Oper State or Aggregate Oper State</td>
<td>Indicates whether this aggregate route is operational and participating in BGP message exchanges.</td>
</tr>
<tr>
<td>Aggregate Metric</td>
<td>The multi-exit discriminator (MED) value configured for this aggregate route. This value is configured through the <code>ip bgp aggregate-address metric</code> command.</td>
</tr>
<tr>
<td>Aggregate Local Preference</td>
<td>The local preference value for this aggregate route. This value is configured through the <code>ip bgp aggregate-address local-preference</code> command.</td>
</tr>
<tr>
<td>Aggregate Community String</td>
<td>The community string value for this aggregate route. This value is configured through the <code>ip bgp aggregate-address community</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip bgp aggregate-address` Creates and deletes a BGP aggregate route.

**MIB Objects**

- `alabgpMIBAggrGroup`
  - `alaBgpAggrSet`
  - `alaBgpAggrLocalPref`
  - `alaBgpAggrMetric`
  - `alaBgpAggrSummarize`
  - `alaBgpAggrCommunity`
**show ip bgp network**

Displays currently defined network configurations.

```
show ip bgp network [ip_address ip_mask]
```

**Syntax Definitions**

- `ip_address`  
  A 32-bit IP address.

- `ip_mask`  
  A 32-bit subnet mask number that determines how many bits of the IP address parameter denote the network number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays all the configured networks, or a single network.

**Examples**

```
-> show ip bgp network
Network                  Mask                      Admin state     Oper state
-------------------------------+-----------------+-------------------------+-------------------------
155.132.1.2               255.255.255.255        disabled      not_active
155.132.1.3               255.255.255.255        disabled      not_active

-> show ip bgp network 155.132.1.2 255.255.255.255
Network address            = 155.132.1.2,
Network mask               = 255.255.255.255,
Network admin state        = disabled,
Network oper state         = not_active,
Network metric             = 0,
Network local preference   = 0,
Network community string   = 0:500 400:1 300:2
```
output definitions

**Network or Network address**
The IP address configured for this local BGP network. This value is configured through the `ip bgp network` command.

**Mask or Network mask**
The mask configured for this local BGP network. This value is configured through the `ip bgp network` command.

**Admin state or Network admin state**
Indicates whether this local BGP network is administratively enabled or disabled. This value is configured through the `ip bgp network admin-state` command.

**Oper state or Network oper state**
Indicates whether this BGP local network is operationally active or inactive.

**Network metric**
The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the `ip bgp network metric` command.

**Network local preference**
The local preference value for this local BGP network. This value is configured through the `ip bgp network local-preference` command.

**Network community string**
The community string value for this local BGP network. This value is configured through the `ip bgp network community` command.

### Release History
Release 7.1.1; command was introduced.

### Related Commands

- **ip bgp network**
  Configures a local BGP network.

### MIB Objects

- **alabgpMIBNetworkGroup**
- **alaBgpNetworkEntry**
**show ip bgp neighbors**

Displays the configured IPv4 BGP peers.

**show ip bgp neighbors [ip_address]**

---

**Syntax Definitions**

\textit{ip\_address} \quad A 32-bit IP address.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

There are two output options for this command. If you specify show ip bgp peer without a peer IP address, then you see summary information for all peers known to the local BGP speaker. If you enter a specific peer IP address with the command, then you see detailed parameter information for that peer only.

---

**Examples**

\texttt{-> show ip bgp neighbors}

Legends: Nbr = Neighbor  
As = Autonomous System  
Nbr address | As | Admin state | Oper state | BGP Id | Up/Down | BFD Status  
----------------+-----+-------------+------------+--------+---------+-------------
192.40.4.29 | 3   | enabled     | estab      | 192.40.4.29 | 00h:14m:48s | disabled   
192.40.4.121 | 5   | disabled    | idle       | 0.0.0.0    | 00h:00m:00s | enabled    

---

**output definitions**

- **Nbr address**: The IP address for this BGP peer. Assign this address through the \texttt{ip bgp neighbor} command.
- **As**: The autonomous system to which this peer belongs. A peer’s AS number is assigned through the \texttt{ip bgp neighbor remote-as} command.
- **Admin state**: Indicates whether this peer has been enabled or disabled through the \texttt{ip bgp neighbor admin-state} command.
- **Oper state**: The current BGP state for this peer. Possible states are \texttt{idle}, \texttt{connect}, \texttt{active}, \texttt{opensent}, \texttt{openconfirm}, and \texttt{established}. 
**output definitions**

<table>
<thead>
<tr>
<th>BgpId</th>
<th>The unique BGP identifier of the peer. This value is configured through the <code>ip bgp neighbor update-source</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up/Down</td>
<td>The time since this peer has transitioned to its current UP or DOWN state. If the peer is currently Established, then this is the time that the peer has been UP. If the peer is currently Idle, then this is the time the peer has been DOWN.</td>
</tr>
<tr>
<td>BFD Status</td>
<td>Indicates whether BFD is enabled or disabled for this peer. The BFD status is configured through the `ip</td>
</tr>
</tbody>
</table>

```
-> show ip bgp neighbors 0.0.0.1
Neighbor address       = 0.0.0.1,
Neighbor autonomous system = 1,
Neighbor Admin state   = enabled,
Neighbor Oper state    = connect,
Neighbor passive status = disabled,
Neighbor name          = peer(0.0.0.1),
Neighbor local address = vlan-215,
Neighbor EBGP multiHop = enabled,
Neighbor next hop self = disabled,
Neighbor TTL security  = 6,
Neighbor Route Refresh = enabled,
Neighbor Ipv4 unicast  = enabled,
Neighbor Ipv4 multicast = disabled,
Neighbor type          = internal,
Neighbor auto-restart  = enabled,
Neighbor route-reflector-client = disabled,
Neighbor confederation status = disabled,
Neighbor remove private AS = disabled,
Neighbor default originate = disabled,
Neighbor maximum prefixes = 5000,
Neighbor max prefixes warning = enabled,
# of prefixes received = 0,
Neighbor MD5 key       = <none>,
Neighbor local port    = 0,
Neighbor TCP window size = 32768
Graceful Restart State = None,
Advertised Restart Interval = 0s,
Forwarding State during restart = NotPreserved,
Activate IPv6 unicast  = enabled,
Configured IPv6 NextHop Address = ::,
Neighbor Ipv6 unicast  = advertised
BFD Status             = Disabled,
Activate IPv4 unicast  = enabled,
BFD Status             = disabled,
Activate IPv4 unicast  = enabled
Activate check-first-AS = enabled
```

**output definitions**

<table>
<thead>
<tr>
<th>Neighbor address</th>
<th>The IP address for this BGP peer. Assign this address through the <code>ip bgp neighbor</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor autonomous system</td>
<td>The autonomous system to which this peer belongs. A peer’s AS number is assigned through the <code>ip bgp neighbor remote-as</code> command.</td>
</tr>
<tr>
<td>output definitions (continued)</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Neighbor Admin state</strong></td>
<td>Indicates whether this peer has been enabled or disabled through the <code>ip bgp neighbor admin-state</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor Oper state</strong></td>
<td>The current BGP state for this peer. Possible states are <strong>idle</strong>, <strong>connect</strong>, <strong>active</strong>, <strong>opensent</strong>, <strong>openconfirm</strong>, and <strong>established</strong>.</td>
</tr>
<tr>
<td><strong>Neighbor passive status</strong></td>
<td>Indicates whether the local BGP speaker is “passive” (i.e., waiting for this peer to initiate a session). This value is configured through the <code>ip bgp neighbor passive</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor name</strong></td>
<td>The name assigned to this peer through the <code>ip bgp neighbor description</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor local address</strong></td>
<td>The interface assigned to this peer. This value is configured through the <code>ip bgp neighbor update-source</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor EBGP multihop</strong></td>
<td>Indicates whether BGP multi-hop support is enabled or disabled. This supports allows external BGP peers to communicate with each other even when they are not directly connected. This value is configured through the <code>ip bgp neighbor ebgp-multihop</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor next hop self</strong></td>
<td>Indicates whether this peer is using next hop processing. This value is configured through the <code>ip bgp neighbor next-hop-self</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor TTL security</strong></td>
<td>Displays the number of hops between the switch and the peer. If the GTSM is disabled the value is displayed as none.</td>
</tr>
<tr>
<td><strong>Neighbor Route Refresh</strong></td>
<td>Indicates whether this peer supports Route Refresh capability as defined in RFC 2918. This capability is an alternative to soft-reconfiguration that can save CPU and memory resources. It allows peers to dynamically request the re-advertisement of BGP routing tables. Since this router supports route refresh all BGP peers are automatically enabled for this capability.</td>
</tr>
<tr>
<td><strong>Neighbor Ipv4 unicast</strong></td>
<td>Indicates whether this peer is multi-protocol IP version 4 unicast capable. This router is IPv4 unicasts capable so all peers will be enabled for this capability.</td>
</tr>
<tr>
<td><strong>Neighbor Ipv4 multicast</strong></td>
<td>Indicates whether this peer is multi-protocol IP version 4 multicast capable. This router is not IPv4 multicasts capable so all peers will be disabled for this capability.</td>
</tr>
<tr>
<td><strong>Neighbor type</strong></td>
<td>Indicates whether this peer is internal or external to the router.</td>
</tr>
<tr>
<td><strong>Neighbor auto-restart</strong></td>
<td>Indicates whether peer auto-restart is enabled or disabled. This value is configured through the <code>ip bgp neighbor auto-restart</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor route-reflector-client</strong></td>
<td>Indicates whether this peer is a client to the local route reflector, if configured. This value is configured through the <code>ip bgp neighbor route-reflector-client</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor confederation status</strong></td>
<td>Indicates whether this peer is a member of a BGP confederation. This value is configured through the <code>ip bgp confederation neighbor</code> command.</td>
</tr>
<tr>
<td><strong>Neighbor remove private AS</strong></td>
<td>Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled. This value is configured through the <code>ip bgp neighbor remove-private-as</code> command.</td>
</tr>
</tbody>
</table>
**Neighbor default originate**
Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises itself as a default to the peer. This value is configured through the `ip bgp neighbor default-originate` command.

**Neighbor maximum prefixes**
The maximum number of prefixes the local router can receive in UPDATE from this peer. This value is configured through the `ip bgp neighbor maximum-prefix` command.

**Neighbor max prefixes warning**
Indicates whether a warning will be issued when this peer exceeds 80 percent of the maximum prefix value. This value is configured through the `ip bgp neighbor update-source` command.

**# of prefixes received**
Displays the total number of prefixes received by this neighbor.

**Neighbor MD5 key [32-47]**
When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured. This value is configured through the `ip bgp neighbor md5 key` command.

**Neighbor local port**
The TCP port used for the session with this peer.

**Neighbor TCP window size**
The size of the TCP window for this BGP session. This value will always be 32768 as that is the maximum size of a BGP message.

**Graceful Restart State**
Indicates the graceful restart state. This feature is not supported in Multiprotocol BGP.

**Advertised Restart Interval**
Indicates the restart interval in seconds.

**Forwarding State during restart**
Indicates whether the peer has preserved the forwarding state during the graceful restart.

**Activate IPv6 unicast**
Indicates if the IPv6 unicast updates are enabled or not. Options include `enabled` or `disabled`.

**Configured IPv6 NextHop Address**
Specifies the IPv6 nexthop address. This is specified using the `ipv6 bgp neighbor ipv6-nexthop` command.

**Neighbor IPv6 unicast**
Indicates whether Multiprotocol IPv6 Unicast capability is enabled or disabled between the peers.

**BFD Status**
Indicates whether BFD is enabled or disabled for this peer. The BFD status is configured through the `ip|ipv6 bgp neighbor bfd-state` command.

**Activate IPv4 unicast**
Indicates if the IPv4 unicast updates are enabled or not for this peer.

**Activate check-first-AS**
Displays the operational status of check for first AS in the ASPATH list.

---

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; BFD Status and Activate IPv4 unicast output fields added.
Release 8.4.1; ‘Neighbor TTL security’ output field added.
Release 8.7 R1; ‘Activate check-first-AS’ output field added.
Related Commands

ip bgp neighbor
ip bgp neighbor ttl-security

MIB Objects

alabgpMIBPeerGroup
  alaBgpPeerAddr
  alaBgpPeerAS
  alaBgpPeerPassive
  alaBgpPeerName
  alaBgpPeerMultiHop
  alaBgpPeerMaxPrefix
  alaBgpPeerMaxPrefixWarnOnly
  alaBgpPeerNextHopSelf
  alaBgpPeerTTLSecurityHops
  alaBgpPeerSoftReconfig
  alaBgpPeerInSoftReset
  alaBgpPeerIpv4Unicast
  alaBgpPeerIpv4Multicast
  alaBgpPeerRcvdRtRefreshMsgs
  alaBgpPeerSentRtRefreshMsgs
  alaBgpPeerRouteMapOut
  alaBgpPeerRouteMapIn
  alaBgpPeerLocalAddr
  alaBgpPeerLastDownReason
  alaBgpPeerLastDownTime
  alaBgpPeerLastReadTime
  alaBgpPeerRcvdNotifyMsgs
  alaBgpPeerSentNotifyMsgs
  alaBgpPeerLastSentNotifyReason
  alaBgpPeerLastRecvNotifyReason
  alaBgpPeerRcvdPrefixes
  alaBgpPeerDownTransitions
  alaBgpPeerType
  alaBgpPeerAutoReStart
  alaBgpPeerClientStatus
  alaBgpPeerConfedStatus
  alaBgpPeerRemovePrivateAs
  alaBgpPeerClearCounter
  alaBgpPeerTTL
  alaBgpPeerAspathListOut
  alaBgpPeerAspathListIn
  alaBgpPeerPrefixListOut
  alaBgpPeerPrefixListIn
  alaBgpPeerCommunityListOut
  alaBgpPeerCommunityListIn
  alaBgpPeerRestart
  alaBgpPeerDefaultOriginate
  alaBgpPeerReconfigureInBound
  alaBgpPeerReconfigureOutBound
  alaBgpPeerMD5Key
  alaBgpPeerMD5KeyEncrypt
  alaBgpPeerRowStatus
  alaBgpPeerUpTransitions
<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>alaBgpPeerLocalIntfName</code></td>
</tr>
<tr>
<td><code>alaBgpPeerCheckFirstAS</code></td>
</tr>
<tr>
<td><code>alaBgpPeerActivateIpv4</code></td>
</tr>
</tbody>
</table>
show ip bgp neighbors policy

Displays BGP peer policy information.

show ip bgp neighbors policy [ip_address]

Syntax Definitions

ip_address A 32-bit IP address.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays all of the configured policies for the router or the polices configured for a specific peer.

Examples

-> show ip bgp neighbors policy
Neighbor address = 0.0.0.0,
    Neighbor autonomous system = 1,
    Neighbor output policy map name = <none>,
    Neighbor input policy map name = <none>,
    Neighbor output aspath-list name = <none>,
    Neighbor input aspath-list name = <none>,
    Neighbor output prefix-list name = <none>,
    Neighbor input prefix-list name = <none>,
    Neighbor output community-list name = <none>,
    Neighbor input community-list name = <none>,
    Neighbor soft reconfiguration = enabled
Neighbor address = 0.0.0.1,
    Neighbor autonomous system = 1,
    Neighbor output policy map name = <none>,
    Neighbor input policy map name = <none>,
    Neighbor output aspath-list name = <none>,
    Neighbor input aspath-list name = <none>,
    Neighbor output prefix-list name = <none>,
    Neighbor input prefix-list name = <none>,
Neighbor output community-list name = <none>,
Neighbor input community-list name = <none>,
Neighbor soft reconfiguration = enabled
Neighbor output prefix6-list name = <none>,
Neighbor input prefix6-list name = <none>

output definitions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor autonomous system</td>
<td>The AS to which the peer is assigned. This can be assigned by using the <code>ip bgp neighbor remote-as</code> command.</td>
</tr>
<tr>
<td>Neighbor output policy map name</td>
<td>The outbound route map policy for the peer. This can be assigned by using the <code>ip bgp neighbor route-map</code> command.</td>
</tr>
<tr>
<td>Neighbor input policy map name</td>
<td>The inbound route map policy for the peer. This can be assigned by using the <code>ip bgp neighbor route-map</code> command.</td>
</tr>
<tr>
<td>Neighbor output aspath-list name</td>
<td>The outbound AS path list policy for the peer. This can be assigned by using the <code>ip bgp neighbor out-aspathlist</code> command.</td>
</tr>
<tr>
<td>Neighbor input aspath-list name</td>
<td>The inbound AS path list policy for the peer. This can be assigned by using the <code>ip bgp neighbor in-aspathlist</code> command.</td>
</tr>
<tr>
<td>Neighbor output prefix-list name</td>
<td>The outbound prefix list policy for the peer. This can be assigned by using the <code>ip bgp neighbor out-prefixlist</code> command.</td>
</tr>
<tr>
<td>Neighbor input prefix-list name</td>
<td>The inbound prefix list policy for the peer. This can be assigned by using the <code>ip bgp neighbor in-prefixlist</code> command.</td>
</tr>
<tr>
<td>Neighbor output community-list name</td>
<td>The outbound community list policy for the peer. This can be assigned by using the <code>ip bgp neighbor out-communitylist</code> command.</td>
</tr>
<tr>
<td>Neighbor input community-list name</td>
<td>The inbound community list policy for the peer. This can be assigned by using the <code>ip bgp neighbor in-communitylist</code> command.</td>
</tr>
<tr>
<td>Neighbor soft reconfiguration</td>
<td>Lists whether soft reconfigurations are enabled or disabled for this peer. This is configured using the <code>ip bgp neighbor soft-reconfiguration</code> command.</td>
</tr>
<tr>
<td>Neighbor output prefix6-list name</td>
<td>The outbound prefix6 list policy for the peer. This can be assigned by using the <code>ip bgp neighbor out-prefix6list</code> command.</td>
</tr>
<tr>
<td>Neighbor input prefix6-list name</td>
<td>The inbound prefix6 list policy for the peer. This can be assigned by using the <code>ip bgp neighbor in-prefix6list</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

- `show ip bgp neighbors` Displays BGP peer main status.
**MIB Objects**

alaBgpPeerTable
- alaBgpPeerAS
- alaBgpPeerRouteMapOut
- alaBgpPeerRouteMapIn
- alaBgpPeerAsPathListOut
- alaBgpPeerAsPathListIn
- alaBgpPeerPrefixListOut
- alaBgpPeerPrefixListIn
- alaBgpPeerCommunityListOut
- alaBgpPeerCommunityListIn
- alaBgpPeerSoftReconfig
- alaBgpPeerPrefix6ListOut
- alaBgpPeerPrefix6ListIn
**show ip bgp neighbors timer**

Displays BGP peer timer statistics.

```
show ip bgp neighbors timer [ip_address]
```

---

### Syntax Definitions

| **ip_address** | A 32-bit IP address. |

---

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

This command displays the timer values for all peer associated with this speaker, or for a specific peer.

### Examples

```
-> show ip bgp neighbors timer
Legends: Nbr = Neighbor
         As  = Autonomous System
         RtAdv = Route Advertisement
         Kalive = Keep Alive (actual)
         Ka(C) = Configured Keep Alive

Nbr address    As    Hold  Hold(C) RtAdv  Retry  Kalive  Ka(C)
---------------+-----+-------+-------+-----+-------+-------+-----+
192.40.4.29    3     90    90      30   120   30    30
192.40.4.121   5     0     90      30   120   0     30
```

---

**output definitions**

- **Nbr address**: The IP address for this BGP peer. Assign this address through the `ip bgp neighbor` command.
- **As**: The autonomous system to which this peer belongs. A peer’s AS number is assigned through the `ip bgp neighbor remote-as` command.
- **Hold**: The current count for the holdtime value.
- **Hold(C)**: The holdtime value configured through the `ip bgp neighbor timers` command.
output definitions (continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RtAdv</td>
<td>The route advertisement interval, in seconds, for updates between external BGP peers. This value is configured through the <code>ip bgp neighbor advertisement-interval</code> command.</td>
</tr>
<tr>
<td>Retry</td>
<td>The interval, in seconds, between retries by this peer to set up a connection through TCP with another peer. This value is configured through the <code>ip bgp neighbor timers</code> command.</td>
</tr>
<tr>
<td>Kalive</td>
<td>The current count, in seconds, between keepalive messages. Keepalive messages do not contain route or status updates; they serve only to tell other peers that the connection is still live and this peer is reachable.</td>
</tr>
<tr>
<td>Ka(C)</td>
<td>The keepalive interval as configured through the <code>ip bgp neighbor timers</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip bgp neighbors` Displays BGP peer main status.

**MIB Objects**

- N/A
**show ip bgp neighbors statistics**

Displays BGP peer message statistics.

`show ip bgp neighbors statistics [ip_address]`

---

**Syntax Definitions**

- `ip_address` A 32-bit IP address.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

This command displays message statistics for all peers associated with this speaker or with a specific peer.

---

**Examples**

```plaintext
-> show ip bgp neighbors statistics
Legends: RMSGS = number of received messages, SMSGS = number of sent messages
RUPDS = number of Update messages received,
SUPDS = number of Update messages sent,
RNOFY = number of Notify messages received,
SNOFY = number of Notify messages sent
RPFXS = number of prefixes received
UPTNS = number of UP transitions
DNTNS = number of DOWN transitions

Nbr address As RMSGS SMSGS RUPDS SUPDS RNOFY SNOFY RPFXS UPTNS DNTNS
----------------------------------------------
192.40.4.29   3   110   123   5     0     0     1     8     2     2
192.40.4.121  5     0     0     0     0     0     0     0     0     0
```

**output definitions**

- **Nbr address** The IP address for this peer. This value is configured through the `ip bgp neighbor` command.
- **As** The autonomous system to which this peer belongs. This value is configured through the `ip bgp neighbor remote-as` command.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>RMSGS</th>
<th>Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMSGS</td>
<td>Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent by this peer.</td>
</tr>
<tr>
<td>RUPDS</td>
<td>The number of route UPDATE messages received by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.</td>
</tr>
<tr>
<td>SUPDS</td>
<td>The number of route UPDATE messages sent by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.</td>
</tr>
<tr>
<td>RNOFY</td>
<td>The number of NOTIFY messages received by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.</td>
</tr>
<tr>
<td>SNOFY</td>
<td>The number of NOTIFY messages sent by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.</td>
</tr>
<tr>
<td>RPFXS</td>
<td>The number of unique route prefixes received by this peer.</td>
</tr>
<tr>
<td>UPTNS</td>
<td>The number of times this peer has come up, operationally.</td>
</tr>
<tr>
<td>DNTNS</td>
<td>Number of times this peer has gone down, operationally.</td>
</tr>
</tbody>
</table>

```
-> show ip bgp neighbors statistics 0.0.0.1
Neighbor address                   = 0.0.0.1,
# of UP transitions                = 0,
Time of last UP transition         = 00h:00m:00s,
# of DOWN transitions              = 0,
Time of last DOWN transition       = 00h:00m:00s,
Last DOWN reason                   = none,
# of msgs rcvd                     = 0,
# of Update msgs rcvd              = 0,
# of prefixes rcvd                 = 0,
# of Route Refresh msgs rcvd       = 0,
# of Notification msgs rcvd        = 0,
Last rcvd Notification reason      = none [none]
Time last msg was rcvd             = 00h:00m:00s,
# of msgs sent                     = 0,
# of Update msgs sent              = 0,
# of Route Refresh msgs sent       = 0
# of Notification msgs sent        = 0,
Last sent Notification reason      = none [none]
Time last msg was sent             = 00h:00m:00s,
```

**output definitions**

<table>
<thead>
<tr>
<th>Neighbor address</th>
<th>The IP address for this peer. This value is configured through the ip bgp neighbor command.</th>
</tr>
</thead>
<tbody>
<tr>
<td># of UP transitions</td>
<td>The number of times this peer has come up, operationally.</td>
</tr>
<tr>
<td>Time of last UP transition</td>
<td>The duration that this peer has been up.</td>
</tr>
<tr>
<td># of DOWN transitions</td>
<td>Number of times this peer has gone down, operationally.</td>
</tr>
<tr>
<td>Time of last DOWN transition</td>
<td>The duration since this peer last went down.</td>
</tr>
</tbody>
</table>
### Last DOWN reason

Provides a message as the last reason why a peer went down. The possible reasons for going down are:

- user_request - user initiated
- conn_timeout - connection timer expired
- hold_timeout - hold timer expired
- bad_msg - received a bad message from neighbor
- fsm_blink - BGP FSM error
- peer_closed - neighbor closed connection
- peer_notify - neighbor sent fatal notification
- tcp_error - Fatal TCP error
- none - None

### # of msgs rcvd

Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received from this peer.

### # of Update msgs rcvd

The number of route UPDATE messages received from this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.

### # of prefixes rcvd

The number of unique route prefixes received by this peer.

### # of Route Refresh msgs rcvd

The number of route refresh requests this peer has received. Route refresh requests all routes learned be a peer.

### # of Notification msgs rcvd

The number of NOTIFY messages received from this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.
### BGP Commands

#### show ip bgp neighbors statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Last rcvd Notification reason</strong></td>
<td>NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message received from this peer. The notification reasons are listed in two parts separated by a dash (-). The following are possible notification reasons:</td>
</tr>
<tr>
<td>message header error - synchronization loss</td>
<td></td>
</tr>
<tr>
<td>message header error - bad length</td>
<td></td>
</tr>
<tr>
<td>message header error - bad type</td>
<td></td>
</tr>
<tr>
<td>open message error - unsupported version</td>
<td></td>
</tr>
<tr>
<td>open message error - bad peer autonomous system</td>
<td></td>
</tr>
<tr>
<td>open message error - bad peer bgp id</td>
<td></td>
</tr>
<tr>
<td>open message error - unsupported option</td>
<td></td>
</tr>
<tr>
<td>open message error - authentication failure</td>
<td></td>
</tr>
<tr>
<td>open message error - unacceptable hold time</td>
<td></td>
</tr>
<tr>
<td>open message error - unsupported capability</td>
<td></td>
</tr>
<tr>
<td>update message error - malformed attribute</td>
<td></td>
</tr>
<tr>
<td>update message error - unknown attribute</td>
<td></td>
</tr>
<tr>
<td>update message error - missing wellknown attribute</td>
<td></td>
</tr>
<tr>
<td>update message error - attribute flags error</td>
<td></td>
</tr>
<tr>
<td>update message error - attribute length error</td>
<td></td>
</tr>
<tr>
<td>update message error - invalid origin</td>
<td></td>
</tr>
<tr>
<td>update message error - as loop</td>
<td></td>
</tr>
<tr>
<td>update message error - invalid nexthop</td>
<td></td>
</tr>
<tr>
<td>update message error - optional attribute error</td>
<td></td>
</tr>
<tr>
<td>update message error - invalid network</td>
<td></td>
</tr>
<tr>
<td>update message error - malformed aspath</td>
<td></td>
</tr>
<tr>
<td>cease - maximum number of prefixes reached</td>
<td></td>
</tr>
<tr>
<td>cease - administrative shutdown</td>
<td></td>
</tr>
<tr>
<td>cease - peer de-configured</td>
<td></td>
</tr>
<tr>
<td>cease - administrative reset</td>
<td></td>
</tr>
<tr>
<td>cease - connection rejected</td>
<td></td>
</tr>
<tr>
<td>cease - other configuration change</td>
<td></td>
</tr>
<tr>
<td>cease - connection collision resolution</td>
<td></td>
</tr>
<tr>
<td>cease - out of resources</td>
<td></td>
</tr>
<tr>
<td>hold time out - none</td>
<td></td>
</tr>
<tr>
<td>fsm error - none</td>
<td></td>
</tr>
<tr>
<td>none - none</td>
<td></td>
</tr>
<tr>
<td><strong>Time last msg was rcvd</strong></td>
<td>The duration since a message was received from this peer.</td>
</tr>
<tr>
<td><strong># of msgs sent</strong></td>
<td>Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent to this peer.</td>
</tr>
<tr>
<td><strong># of Update msgs sent</strong></td>
<td>The number of route UPDATE messages sent to this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.</td>
</tr>
<tr>
<td><strong># of Route Refresh msgs sent</strong></td>
<td>The number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer.</td>
</tr>
<tr>
<td><strong># of Notification msgs sent</strong></td>
<td>The number of NOTIFY messages sent to this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

| Last sent Notification reason | NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message sent by this peer. The notification reasons are listed in two parts separated by a dash (-). See the list of possible notification reasons under the description for the Peer last received notification reason field above. |
| Time last msg was sent | The duration since a message was sent to this peer. |

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip bgp neighbor** Creates or deletes a BGP peer.

**MIB Objects**

- N/A
show ip bgp policy aspath-list

Displays AS path list parameters.

show ip bgp policy aspath-list [name] ["regular_expression"]

Syntax Definitions

name
An AS path name.

regular_expression
A regular expression. The regular expression must be enclosed by quotation marks.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command displays a list of all of the AS path policies for the router, or a single policy selected by the list name or regular expression.

- Regular expressions are defined in the ip bgp policy aspath-list command on page 30-136.

- When using regular expressions in the CLI, the regular expression must be enclosed by quotation marks.

Examples

- show ip bgp policy aspath-list
  Aspath List Name Aspath regular expression
  --------------------+--------------------------------------------------
  aspl1              (500 | 400) ? 300$
  aspl2              (500 | 400)

- show ip bgp policy aspath-list aspl1
  Aspath List name = aspl1
  Aspath Regexp      = (500 | 400) ? 300$
  Admin state        = disabled,
  Priority           = 1,
  Action             = deny,
  Primary index      = 0,
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASPATH LIST NAME</td>
<td>The name of the AS path list. This is defined using the <code>ip bgp policy aspath-list</code> command.</td>
</tr>
<tr>
<td>ASPATH REGULAR EXPRESSION</td>
<td>The regular expression that defines the AS path list. This is defined using the <code>ip bgp policy aspath-list</code> command.</td>
</tr>
<tr>
<td>ADMIN STATE</td>
<td>The administration state of the AS path policy. It is either enable or disable.</td>
</tr>
<tr>
<td>PRIORITY</td>
<td>The AS path list priority. This is defined using the <code>ip bgp policy aspath-list priority</code> command.</td>
</tr>
<tr>
<td>ACTION</td>
<td>The AS path list action, either permit or deny. This is defined using the <code>ip bgp policy aspath-list action</code> command.</td>
</tr>
<tr>
<td>PRIMARY INDEX</td>
<td>The instance identifier for the AS path list. This value is not configurable.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

`ip bgp policy aspath-list` Creates or removes an AS path list.

MIB Objects

`alabgpMIBAspathListGroup`
- `alaBgpAspathMatchListId`
- `alaBgpAspathMatchListRegExp`
- `alaBgpAspathMatchListPriority`
- `alaBgpAspathMatchListAction`
- `alaBgpAspathMatchListRowStatus`
**show ip bgp policy community-list**

Displays community list parameters.

```
show ip bgp policy community-list [name] [string]
```

### Syntax Definitions

- **name**
  Community name.

- **string**
  A regular expression. The regular expression must be enclosed by quotation marks.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays a list of the community policies for the speaker, or a specific policy defined by its name or community match string.

### Examples

```
-> show ip bgp policy community-list
Community list name    Community string
------------------------+-----------------------------------------
 adfasdf                0:0

-> show ip bgp policy community-list comll
 Community List name = comll
 Community string = 600:1
  Admin state = disabled,
  Match type = exact,
  Priority = 1,
  Action = deny,
  Primary index = 0
```
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community List name</td>
<td>The community list name. This is defined using the ip bgp policy community-list command.</td>
</tr>
<tr>
<td>Community string</td>
<td>The community list definition. This is defined using the ip bgp policy community-list command.</td>
</tr>
<tr>
<td>Admin state</td>
<td>The administration state of the community list policy, either enabled or disabled.</td>
</tr>
<tr>
<td>Match type</td>
<td>The match type of the community list. This is defined using the ip bgp policy community-list match-type command.</td>
</tr>
<tr>
<td>Priority</td>
<td>The community list priority. This is defined using the ip bgp policy community-list priority command.</td>
</tr>
<tr>
<td>Action</td>
<td>The community list action. This is defined using the ip bgp policy community-list action command.</td>
</tr>
<tr>
<td>Primary index</td>
<td>The instance identifier for the community list. This value is not configurable.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

ip bgp policy community-list Creates or deletes a community list.

MIB Objects

alabgpMIBCommunityListGroup
  alaBgpCommunityMatchListId
  alaBgpCommunityMatchListString
  alaBgpCommunityMatchListPriority
  alaBgpCommunityMatchListType
  alaBgpCommunityMatchListActionCode
  alaBgpCommunityMatchListRowStatus
show ip bgp policy prefix-list

Displays prefix list parameters.

`show ip bgp policy prefix-list [name] [ip_address ip_mask]`

**Syntax Definitions**

- **name**: A prefix list name.
- **ip_address**: A prefix list IP address.
- **ip_mask**: An IP address mask.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the list of prefix-list policies configured for the speaker, or a specific list determined by the list name or IP address and mask.

**Examples**

```
-> show ip bgp policy prefix-list
Prefix List name          Prefix address  Prefix mask
-------------------------------+---------------+---------------
pfx11                    155.132.33.0    255.255.255.0
pfx12                    155.148.32.0    255.255.255.0

-> show ip bgp policy prefix-list pfx11
Prefix List name = pfx11
Address = 155.132.33.0
Mask = 255.255.255.0
Admin state = disabled,
Match Mask >= (GE) = 0,
Match Mask <= (LE) = 0,
```
<table>
<thead>
<tr>
<th>Action</th>
<th>= deny</th>
</tr>
</thead>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Prefix List name</th>
<th>The name of the prefix list. This is defined using the <code>ip bgp policy prefix-list</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The IP address of the prefix list. This is defined using the <code>ip bgp policy prefix-list</code> command.</td>
</tr>
<tr>
<td>Mask</td>
<td>The mask of the prefix list. This is defined using the <code>ip bgp policy prefix-list</code> command.</td>
</tr>
<tr>
<td>Admin state</td>
<td>The administrative state of the prefix list, either enabled or disabled.</td>
</tr>
<tr>
<td>Match Mask &gt;= (GE)</td>
<td>The GE match mask of the prefix list. This is defined using the <code>ip bgp policy prefix-list ge</code> command.</td>
</tr>
<tr>
<td>Match Mask &lt;= (LE)</td>
<td>The GE match mask of the prefix list. This is defined using the <code>ip bgp policy prefix-list le</code> command.</td>
</tr>
<tr>
<td>Action</td>
<td>The action of the prefix list. This is defined using the <code>ip bgp policy prefix-list action</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`ip bgp policy prefix-list` Creates or deletes a prefix match list.

**MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alabgpMIBPrefixListGroup</td>
</tr>
<tr>
<td>alabgpPrefixMatchListId</td>
</tr>
<tr>
<td>alabgpPrefixMatchListAddr</td>
</tr>
<tr>
<td>alabgpPrefixMatchListMask</td>
</tr>
<tr>
<td>alabgpPrefixMatchListGE</td>
</tr>
<tr>
<td>alabgpPrefixMatchListLE</td>
</tr>
<tr>
<td>alabgpPrefixMatchListAction</td>
</tr>
<tr>
<td>alabgpPrefixMatchListRowStatus</td>
</tr>
</tbody>
</table>
**show ip bgp policy prefix6-list**

Displays prefix6 list parameters.

```
show ip bgp policy prefix6-list [name] [ipv6_address/prefixLength]
```

### Syntax Definitions

- **name**: A prefix6 list name.
- **ip_address**: A prefix6 list IPv6 address.
- **prefixLength**: A prefix6 list prefix length.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

This command displays the list of prefix6-list policies configured for the speaker, or a specific list determined by the list name or IPv6 address.

### Examples

```
-> show ip bgp policy prefix6-list
Prefix6 List name  Prefix6 address/Prefix length
-----------------------------------------------
p62                ::/0
p63                4001:1::/32

-> show ip bgp policy prefix6-list p63
Prefix6 List name  = p63
Prefix             = 4001:1::
Prefix Length      = 32
Admin state        = enabled,
Match MaskLength   = (GE) = 32,
Match MaskLength   = (LE) = 0,
```
BGP Commands

show ip bgp policy prefix6-list

Action             = permit

output definitions

Prefix6 List name  The name of the prefix6 list. This is defined using the \texttt{ip bgp policy prefix6-list} command.
Prefix             The IPv6 address of the prefix6 list. This is defined using the \texttt{ip bgp policy prefix6-list} command.
Prefix Length      The prefix length of the prefix6 list. This is defined using the \texttt{ip bgp policy prefix6-list} command.
Admin state        The administrative state of the prefix6 list, either enabled or disabled.
Match MaskLength $\geq$ (GE) The GE match masklength of the prefix6 list. This is defined using the \texttt{ip bgp policy prefix6-list} command.
Match MaskLength $\leq$ (LE) The LE match masklength of the prefix6 list. This is defined using the \texttt{ip bgp policy prefix6-list} command.
Action             The action of the prefix6 list. This is defined using the \texttt{ip bgp policy prefix6-list} command.

Release History
Release 7.1.1; command was introduced.

Related Commands

\texttt{ip bgp policy prefix6-list} Creates or deletes a prefix6 match list.

MIB Objects

\texttt{alaBgpPrefix6MatchListTable}
  \texttt{alaBgpPrefix6MatchListId}
  \texttt{alaBgpPrefix6MatchListAddr}
  \texttt{alaBgpPrefix6MatchListAddrLength}
  \texttt{alaBgpPrefix6MatchListGE}
  \texttt{alaBgpPrefix6MatchListLE}
  \texttt{alaBgpPrefix6MatchListAction}
  \texttt{alaBgpPrefix6MatchListRowStatus}
show ip bgp policy route-map

Displays policy route map parameters.

\texttt{show ip bgp policy route-map [name] [sequence\_number]}

**Syntax Definitions**

- **name**: Route map name.
- **sequence\_number**: A sequence number. The valid range is 1–255.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C8/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The route map is displayed as a summary table by entering only the route map name, or as a detailed list by specifying the sequence number.

**Examples**

- `-> show ip bgp policy route-map`
  RouteMap name Instance
  ---------------------------+-------
  rmap1                      1
  rmap1                      2
  rmap2                      1

- `-> show ip bgp policy route-map rmap1`
  RouteMap name = rmap1
  RouteMap instance = 1
  Admin state = disabled,
  Local pref (mode/value) = <none> / 0,
  Route map action = permit,
  Origin = <none>,
  MED (mode/value) = <none> / 0,
  Weight = 0,
  Aspath-List name = aspl1,
  Aspath prepend = <none>,
  Aspath match primitive = 500 .* 400$,
  Prefix-List name = <none>,
  <none>
Prefix match primitive = 0.0.0.0 0.0.0.0,
Prefix6-List name = <none>,
Prefix6 match primitive = ::/0,
Prefix6-List name = <none>,
Prefix6 match primitive = ::/0,
Community-list name = coml2,
Community match primitive = <none>,
Community string [mode] = [Additive]

output definitions

<table>
<thead>
<tr>
<th>RouteMap name</th>
<th>The name of the route map policy. This is determined using the <code>ip bgp policy prefix6-list</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RouteMap instance</td>
<td>The instance of the route map policy. This is determined using the <code>ip bgp policy prefix6-list</code> command.</td>
</tr>
<tr>
<td>Admin state</td>
<td>The administrative state of the route map policy, either enabled or disabled.</td>
</tr>
<tr>
<td>Local pref (mode/value)</td>
<td>The local preference of the route map policy. This is determined using the <code>ip bgp policy route-map lpref</code> command.</td>
</tr>
<tr>
<td>Route map action</td>
<td>The action of the route map policy. This is determined using the <code>ip bgp policy route-map action</code> command.</td>
</tr>
<tr>
<td>Origin</td>
<td>The origin of the route map policy. This is determined using the <code>ip bgp policy route-map origin</code> command.</td>
</tr>
<tr>
<td>MED (mode/value)</td>
<td>The MED of the route map policy. This is determined using the <code>ip bgp policy route-map med</code> command.</td>
</tr>
<tr>
<td>Weight</td>
<td>The weight of the route map policy. This is determined using the <code>ip bgp policy route-map weight</code> command.</td>
</tr>
<tr>
<td>Aspath-List name</td>
<td>The name of the AS path list attached to this route map. This is set using the <code>show ip bgp policy aspath-list</code> command.</td>
</tr>
<tr>
<td>Aspath prepend</td>
<td>The value to prepend to the AS_PATH attribute of the routes matched by this RouteMap instance (Empty quotes indicates no AS_PATH prepending is to be done).</td>
</tr>
<tr>
<td>Aspath match primitive</td>
<td>The regular expression used to match AS Path for this route map.</td>
</tr>
<tr>
<td>Prefix-List name</td>
<td>The name of the prefix list attached to this route map. This is set using the <code>show ip bgp policy prefix-list</code> command.</td>
</tr>
<tr>
<td>Prefix match primitive</td>
<td>The prefix to match for this route map.</td>
</tr>
<tr>
<td>Prefix6-List name</td>
<td>The name of the prefix6 list attached to this route map.</td>
</tr>
<tr>
<td>Prefix6 match primitive</td>
<td>The prefix6 to match for this route map.</td>
</tr>
<tr>
<td>Community-List name</td>
<td>The name of the community list attached to this route map. This is set using the <code>show ip bgp policy community-list</code> command.</td>
</tr>
<tr>
<td>Community match primitive</td>
<td>The community string to match for this route map.</td>
</tr>
<tr>
<td>Community string [mode]</td>
<td>The name of the community mode attached to this route map. This is set using the <code>ip bgp policy route-map community-mode</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; “Prefix6-List name” and “Prefix6 match primitive” output fields added.
**Related Commands**

*ip bgp policy route-map*  Creates or deletes a policy route map.

**MIB Objects**

alabgpMIBRouteMapGroup
- alaBgpRouteMapName
- alaBgpRouteMapInst
- alaBgpRouteMapAsPathMatchListId
- alaBgpRouteMapPrefixMatchListId
- alaBgpRouteMapCommunityMatchListId
- alaBgpRouteMapOrigin
- alaBgpRouteMapLocalPref
- alaBgpRouteMapLocalPrefMode
- alaBgpRouteMapMed
- alaBgpRouteMapMedMode
- alaBgpRouteMapAsPrepend
- alaBgpRouteMapSetCommunityMode
- alaBgpRouteMapCommunity
- alaBgpRouteMapMatchAsRegExp
- alaBgpRouteMapMatchPrefix
- alaBgpRouteMapMatchMask
- alaBgpRouteMapMatchCommunity
- alaBgpRouteMapWeight
- alaBgpRouteMapAction
- alaBgpRouteMapRowStatus
- alaBgpRouteMapPrefix6MatchListId
- alaBgpRouteMapMatchPrefix6
- alaBgpRouteMapMatchMaskLength6
**ip bgp graceful-restart**

Configures support for the graceful restart feature on a BGP router.

```
ip bgp graceful-restart
no ip bgp graceful-restart
```

---

**Syntax Definitions**

N/A

**Defaults**

Graceful restart is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable support for the graceful restart feature on a BGP router. It has only unplanned graceful restart.
- The minimum hardware configuration for this command is a redundant CMM configuration.
- Note that graceful restart does not support IPv6 prefixes at this time.

**Examples**

```
-> ip bgp graceful restart
-> no ip bgp graceful restart
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

`show ip bgp`  
Displays the current global settings for the local BGP speaker.

**MIB Objects**

`alaBgpGlobal`  
- `alaBgpGracefulRestart`
- `alaBgpRestartInterval`
**ip bgp graceful-restart restart-interval**

Configures the grace period for achieving a graceful BGP restart.

```
ip bgp graceful-restart restart-interval [seconds]
```

**Syntax Definitions**

- **seconds**: The hitless restart timeout interval, in seconds. The valid range is 1–3600.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>90</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C6/EV48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The minimum hardware configuration for this command is a redundant CMM configuration.
- Note that graceful restart does not support IPv6 prefixes at this time.

**Examples**

```
-> ip bgp graceful-restart restart-interval 600
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show ip bgp**: Displays the current global settings for the local BGP speaker.

**MIB Objects**

- **alaBgpGlobal**
  - **alaBgpGracefulRestart**
  - **alaBgpRestartInterval**
**ip bgp unicast**

Enables or disables unicast IPv4 advertisements for the BGP routing process.

```plaintext
ip bgp unicast
no ip bgp unicast
```

---

**Syntax Definitions**

N/A

---

**Defaults**

By default, BGP IPv4 advertisements are enabled.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to turn off IPv4 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv4 unicast advertisements.
- IPv4 unicast advertisements may be turned off on homogeneous IPv6 networks that are not aware of IPv4 routing. In such cases, the command, **ip router router-id**, must be used to explicitly configure the 32-bit unique router identifier.

---

**Examples**

```plaintext
-> ip bgp unicast
-> no ip bgp unicast
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ipv6 bgp unicast**: Enables or disables unicast IPv6 updates for the BGP routing process.
- **show ip bgp**: Displays the current global settings for the local BGP speaker.
- **ip router router-id**: Configures the router ID for the router.

MIB Objects

- **alaBgpGlobal**
  - **alaBgpMultiProtocolIpv4**
ipv6 bgp unicast

Enables or disables unicast IPv6 advertisements for the BGP routing process.

ipv6 bgp unicast

no ipv6 bgp unicast

Syntax Definitions

N/A

Defaults

By default, IPv6 BGP advertisements are disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to turn off IPv6 unicast advertisements.
- BGP should be disabled before enabling or disabling IPv6 unicast advertisements.

Examples

-> ipv6 bgp unicast
-> no ipv6 bgp unicast

Release History

Release 7.1.1; command was introduced.

Related Commands

- ip bgp unicast Enables or disables unicast IPv4 updates for the BGP routing process.
- show ip bgp Displays the current global settings for the local BGP speaker.

MIB Objects

- alaBgpGlobal
  - alaBgpMultiProtocolIpv6
**ip bgp neighbor activate-ipv6**

Enables or disables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

**ip bgp neighbor ip_address activate-ipv6**

**no ip bgp neighbor ip_address activate-ipv6**

---

**Syntax Definitions**

*ip_address*  
The 32-bit IPv4 address of the neighbor.

**Defaults**

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **no** form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv4 addresses.

**Examples**

```
-> ip bgp neighbor 1.0.0.1 activate-ipv6
-> no ip bgp neighbor 1.0.0.1 activate-ipv6
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

*show ip bgp neighbors*  
Displays BGP peer main status.

**MIB Objects**

alaBgpPeerTable

alaBgpPeerAddr

alaBgpPeerIpv6Unicast
**ip bgp neighbor ipv6-nexthop**

Configures the IPv6 next hop addresses for the IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv4 addresses.

```
ip bgp neighbor ip_address ipv6-nexthop ipv6_address
```

**Syntax Definitions**

- `ip_address`: The 32-bit IPv4 address of the neighbor.
- `ipv6_address`: A 128-bit global IPv6 address to be used as the next hop for IPv6 routes being advertised to this BGP speaker.

**Defaults**

By default, the IPv6 next hop value is set to all zeros.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer `next-hop-self` option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.

**Examples**

- `-> ip bgp neighbor 1.0.0.1 ipv6-nexthop 2001:100:3:4::1`
- `-> ip bgp neighbor 1.0.0.1 ipv6-nexthop ::`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ipv6 bgp neighbors` Displays the configured IPv6 BGP peers.

**MIB Objects**

- `alaBgpPeerTable`
- `alaBgpPeerAddr`
ip bgp neighbor ipv6-next-hop

#### alaBgpPeerIpv6NextHop
**show ipv6 bgp path**

Displays the known IPv6 BGP paths for all the routes or a specific route.

`show ipv6 bgp path [ipv6-address/prefix_length] [detail]`

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address.
- `/prefix_length`: The number of bits that are significant in the IPv6 address (mask) (3..128).

**Defaults**

By default, IPv6 BGP paths for all the routes will be displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `ipv6_address/prefix_length` parameter to display the IPv6 BGP paths for a specified route.
- Use the `detail` option to display the AS Path details of each route.

**Examples**

```plaintext
-> show ipv6 bgp path
Legends: Sta = Path state
         > = best, F = feasible, S = stale
         U = un-synchronized
         Nbr = Neighbor
         (O) = Path Origin (? = incomplete, i = igp, e = egp)
         degPref = degree of preference
Sta  Prefix                        Nbr Address                         (O) degPref
---+-----------------------------+------------------------------------+---+-------
>  2020:100:200:1::/64           2001:100:3:4::1                      i   100
>  2020:100:200:2::/64           2001:100:3:4::1                      i   100
>  2020:100:200:3::/64           2001:100:3:4::1                      i   100
>  2020:100:200:4::/64           2001:100:3:4::1                      i   100
>  2020:100:200:5::/64           2001:100:3:4::1                      i   100
>  2525:2525:1::/48              100.3.4.1                           i   100
>  2525:2525:2::/48              100.3.4.1                           i   100
>  2525:2525:3::/48              100.3.4.1                           i   100
>  2525:2525:4::/48              100.3.4.1                           i   100
>  2525:2525:5::/48              100.3.4.1                           i   100
```
-> show ipv6 bgp path detail
Legends: Sta = Path state
       > = best, F = feasible, S = stale
       Nbr = Neighbor
       (O) = Path Origin (? = incomplete, i = igp, e = egp)
       degPref = degree of preference

<table>
<thead>
<tr>
<th>Sta</th>
<th>Prefix</th>
<th>Nbr address</th>
<th>degPref</th>
<th>AS Path, (O)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt;</td>
<td>3001:1::/64</td>
<td>2001:1::2</td>
<td>100</td>
<td>65535 65530, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>3001:1:0:1::/64</td>
<td>2001:1::2</td>
<td>100</td>
<td>65535 65530, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>3001:1:0:2::/64</td>
<td>2001:1::2</td>
<td>100</td>
<td>65535 65530, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>4001:1:0:1::/64</td>
<td>2101::51</td>
<td>140</td>
<td>65536, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>4001:1:0:2::/64</td>
<td>2101::51</td>
<td>140</td>
<td>65536, i</td>
</tr>
<tr>
<td>&gt;</td>
<td>4001:1:0:3::/64</td>
<td>2101::51</td>
<td>140</td>
<td>65536, i</td>
</tr>
</tbody>
</table>

output definitions

Sta
Status flag. A greater-than sign (>) indicates this is the best route to the destination.

Prefix
The destination address of the IPv6 route in the hexadecimal format.

Nbr Address
The IP or IPv6 address of the BGP peer that advertises this path.

(0)
The origin attribute of this route path. A question mark (?) indicates incomplete, and i indicates IGP, and an e indicates EGP.

degPref
The local preference value assigned to this route path.

-> show ipv6 bgp path ipv6-addr 2020:100:200:1::/64
BGP Path parameters
Path address = 2020:100:200:1::
Path Length = 64
Path protocol = ibgp
Path neighbor = peer(2001:100:3:4::1)
  Path nextHop = 2001:100:3:4::1,
  Path origin = igp,
  Path local preference = 100,
  Path state = active,
  Path weight = 0,
  Path preference degree = 100,
  Path autonomous systems = [nAs=0] : <none>,
  Path MED = <none>,
  Path atomic = no,
  Path AS aggregator = <none>,
  Path IPaddr aggregator = <none>,
  Path community = <none>,
  Path Originator Id = <none>,
  Path Cluster List = <none>,
  Path unknown attribute = <none>

output definitions

Path address
The IPv6 address for route path.

Path Length
The prefix length of the IPv6 path.

Path protocol
The protocol from which this route path was learned. Possible values for this field are as follows: local, static, directhost, rip, ospf, isis, ibgp, ebgp, and other.

Path neighbor
The IPv6 address of the BGP peer.
output definitions (continued)

<table>
<thead>
<tr>
<th>Path nextHop</th>
<th>The next hop along the route path.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path origin</td>
<td>The BGP origin attribute. Possible values will be <strong>igp</strong>, <strong>egp</strong>, <strong>incomplete</strong>, and <strong>none</strong>. The origin attribute is considered during the route decision process.</td>
</tr>
<tr>
<td>Path local preference</td>
<td>The local preference value for this route as received in an UPDATE message. A negative value (for example, the <strong>-1</strong> in the above display) indicates that the local preference value is missing for this route path.</td>
</tr>
<tr>
<td>Path state</td>
<td>Indicates the state of the path. The possible states are <strong>best</strong>, <strong>feasible</strong>, <strong>policy-wait</strong>, <strong>un-synchronized</strong>, <strong>dampened</strong>, or <strong>none</strong>. When path state is <strong>none</strong>, it indicates that there are no paths to this prefix and the route is being purged from the system.</td>
</tr>
<tr>
<td>Path weight</td>
<td>The path weight as assigned through inbound and outbound policies.</td>
</tr>
<tr>
<td>Path preference degree</td>
<td>The local preference assigned to this route through an inbound or outbound policy, or, if the local preference value is missing, the default local preference (which is assigned through the <strong>ip bgp default local-preference</strong>).</td>
</tr>
<tr>
<td>Path autonomous systems</td>
<td>The AS path for this route. These numbers show the ASs through which the route has traversed with the most recent AS listed first. In the above example, this route began its path in AS 2 and then traveled through AS 3.</td>
</tr>
<tr>
<td>Path MED</td>
<td>The multi-exit discriminator (MED) value for this route path. A negative value (for example, the <strong>-1</strong> in the above display) indicates that the MED value is missing for this route path.</td>
</tr>
<tr>
<td>Path atomic</td>
<td>Indicates whether the ATOMIC-AGGREGATE attribute has been set for this route. When set (this field would read <strong>yes</strong>), this attribute indicates that an aggregate has caused a loss of information for this route (a less specific route was chosen over a more specific route included in the aggregate).</td>
</tr>
<tr>
<td>Path AS aggregator</td>
<td>Part of the AGGREGATOR attribute. This field indicates the AS for the BGP speaker that created the aggregate. A value of <strong>&lt;none&gt;</strong> indicates this is not an aggregate route.</td>
</tr>
<tr>
<td>Path IPaddr aggregator</td>
<td>Part of the AGGREGATOR attribute. This field indicates the IP address for the BGP speaker that created the aggregate. A value of <strong>&lt;none&gt;</strong> indicates that this is not an aggregate route.</td>
</tr>
<tr>
<td>Path community</td>
<td>Indicates the community to which this route path belongs, if applicable. A value of <strong>&lt;none&gt;</strong> indicates that this route does not belong to a community.</td>
</tr>
<tr>
<td>Path Originator Id</td>
<td>The Router Id of the BGP4 speaker that performed route reflection</td>
</tr>
<tr>
<td>Path Cluster List</td>
<td>Sequence of Cluster Id values representing the reflection path that the route has passed, if this is a reflected route in the local AS.</td>
</tr>
<tr>
<td>Path unknown attribute</td>
<td>Indicates BGP attributes found in UPDATE messages which the router does not support. For example, multi-protocol attributes are not supported by the router in this release, but it is possible for these attributes to appear in a BGP route.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; `detail` keyword added.

**Related Commands**

- `show ipv6 bgp routes` Displays the known IPv6 BGP routes.

**MIB Objects**

- `alaBgpPath6Table`  
  - `alaBgpPath6Addr`  
  - `alaBgpPath6MaskLen`  
  - `alaBgpPath6PeerBgpId`  
  - `alaBgpPath6SrcProto`  
  - `alaBgpPath6Weight`  
  - `alaBgpPath6Pref`  
  - `alaBgpPath6State`  
  - `alaBgpPath6Origin`  
  - `alaBgpPath6NextHop`  
  - `alaBgpPath6As`  
  - `alaBgpPath6LocalPref`  
  - `alaBgpPath6Med`  
  - `alaBgpPath6Atomic`  
  - `alaBgpPath6AggregatorAs`  
  - `alaBgpPath6AggregatorAddr`  
  - `alaBgpPath6Community`  
  - `alaBgpPath6OriginatorId`  
  - `alaBgpPath6ClusterList`  
  - `alaBgpPath6PeerName`  
  - `alaBgpPath6UnknownAttr`
show ipv6 bgp routes

Displays the known IPv6 BGP routes.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 bgp routes

Legends: ECL = EBGP change list, ICC = IBGP client change list
ICL = IBGP change list, LCL = local change list
AGG = Aggregation, AGC = Aggregation contribution
AGL = Aggregation list, GDL = Deletion list
AGW = Aggregation waiting, AGH = Aggregation hidden
DMP = Dampening, ACT = Active route

<table>
<thead>
<tr>
<th>Prefix</th>
<th>ECL</th>
<th>ICC</th>
<th>ICL</th>
<th>LCL</th>
<th>AGG</th>
<th>AGC</th>
<th>AGL</th>
<th>AGW</th>
<th>AGH</th>
<th>GDL</th>
<th>DMP</th>
<th>ACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020:100:200:1::/64</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2020:100:200:2::/64</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2020:100:200:3::/64</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2020:100:200:4::/64</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2020:100:200:5::/64</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2525:2525:1::/48</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2525:2525:2::/48</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2525:2525:3::/48</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

output definitions

Prefix                          | The destination address of the IPv6 route in the hexadecimal format.
ECL                             | External BGP change list. When Yes, this route will be advertised as soon as the route advertisement timer expires.
output definitions (continued)

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICC</td>
<td>Internal BGP client change list. When Yes, this route will be advertised to internal non-clients.</td>
</tr>
<tr>
<td>ICL</td>
<td>Internal BGP change list. When Yes, this route has changes that need to be advertised.</td>
</tr>
<tr>
<td>LCL</td>
<td>Local change list. When Yes, this route is local.</td>
</tr>
<tr>
<td>AGG</td>
<td>Aggregation. When Yes, this route is an aggregate route.</td>
</tr>
<tr>
<td>AGC</td>
<td>Aggregation contribution. When Yes, this route is part of an aggregate route.</td>
</tr>
<tr>
<td>AGL</td>
<td>Aggregation list. When Yes, this route is placed on an aggregate list.</td>
</tr>
<tr>
<td>AGW</td>
<td>Aggregation waiting. When Yes, this route is waiting for an aggregate contributor.</td>
</tr>
<tr>
<td>AGH</td>
<td>Aggregation hidden. When Yes, this route is hidden as part of an aggregate route.</td>
</tr>
<tr>
<td>GDL</td>
<td>Deletion list. When Yes, this route will be deleted.</td>
</tr>
<tr>
<td>DMP</td>
<td>Dampening. Indicate whether this route has been dampened. If ‘Yes’, then this route has been dampened and a dampening history exists.</td>
</tr>
<tr>
<td>ACT</td>
<td>Active route. When Yes, the route is active.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

```
show ipv6 bgp path
```

Displays the known IPv6 BGP paths for all the routes or a specific route.

MIB Objects

```
alaBgpRoute6Table
   alaBgpRoute6Addr
   alaBgpRoute6MaskLen
   alaBgpRoute6State
   alaBgpRoute6IsHidden
   alaBgpRoute6IsAggregate
   alaBgpRoute6IsAggregateContributor
   alaBgpRoute6IsAggregateList
   alaBgpRoute6IsAggregateWait
   alaBgpRoute6IsOnEbgpChgList
   alaBgpRoute6IsOnIbgpClientChgList
   alaBgpRoute6IsOnIbgpChgList
   alaBgpRoute6IsOnLocalChgList
   alaBgpRoute6IsOnDeleteList
   alaBgpRoute6IsDampened
```
### ipv6 bgp network

Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

**ipv6 bgp network ipv6_address/prefix_length**

**no ipv6 bgp network ipv6_address/prefix_length**

---

**Syntax Definitions**

- **ipv6_address**
  - The 128-bit IPv6 address.

- **/prefix_length**
  - The number of bits that are significant in the IPv6 address (mask) (3..128).

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the **no** form of this command to turn off the advertisement of locally reachable IPv6 networks.

---

**Examples**

`-> ipv6 bgp network 2001::1/64`

`-> no ipv6 bgp network 2001::1/64`

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- **ipv6 bgp network admin-state**
  - Enables or disables a BGP network.

- **show ipv6 bgp network**
  - Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

---

**MIB Objects**

- alaBgpNetwork6Table
- alaBgpNetwork6Addr
ipv6 bgp network

```plaintext
       1 2 3 4
        |---|
       0 1 2 3
        |   |
IPv6 Format:

   a1aBgpNetwork6MaskLen
```

---

BGP Commands

---
**ipv6 bgp network community**

 Defines a community for a route created by the `ipv6 bgp network` command. Communities are a way of grouping BGP peers that do not share an IPv6 subnet or an AS.

```
ipv6 bgp network ipv6_address/prefix_length [community {none | no-export | no-advertise | no-export-subconfed | num | num:num}]
```

**Syntax Definitions**

- `ipv6_address`  
  The 128-bit IPv6 address.

- `/prefix_length`  
  The number of bits that are significant in the IPv6 address (mask). The valid range is 3–128

- `none`  
  Removes a prefix from a community.

- `no-export`  
  Routes in this community are advertised within the AS but not beyond the local AS.

- `no-advertise`  
  Routes in this community are not advertised to any peer.

- `no-export-subconfed`  
  Routes in this community are not advertised to any external BGP peer.

- `num`  
  The community attribute number.

- `num:num`  
  Community attribute in the AS:NN format. AS indicates the autonomous system and NN indicates the community number.

**Defaults**

By default, a route is not assigned to a community.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The IPv6 BGP route created with the `ipv6 bgp network` command should exist before the community attribute is defined.

- The value of AS:NN is num:num:num if using asdot or asdot+ notation and is num:num if using asplain format.

**Examples**

```
-> ipv6 bgp network 2004::2/64 community 23:20
```
Release History

Release 7.1.1; command was introduced.
Release 7.3.4; syntax added to community string.

Related Commands

`ipv6 bgp network`  Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

`show ipv6 bgp network`  Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

MIB Objects

alaBgpNetwork6Table
  - alaBgpNetwork6Addr
  - alaBgpNetwork6MaskLen
  - alaBgpNetwork6Community
**ipv6 bgp network local-preference**

Defines the local preference value for a route generated by the `ipv6 bgp network` command. This value will override the default local preference value; it is used when announcing this network to internal peers.

```
ipv6 bgp network ipv6_address/prefix_length [local-preference num]
```

### Syntax Definitions

- **ipv6_address**
  - The 128-bit IPv6 address.

- **/prefix_length**
  - The number of bits that are significant in the IPv6 address (mask) (3..128).

- **num**
  - The local preference attribute value. The valid range is 0–4294967295.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The IPv6 BGP route created with the `ipv6 bgp network` command should exist before the `local-preference` attribute is defined.

### Examples

```
-> ipv6 bgp network 2004::1/24 local-preference 6
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **ipv6 bgp network**  Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers
- **show ipv6 bgp network**  Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

**MIB Objects**

alaBgpNetwork6Table
  - alaBgpNetwork6Addr
  - alaBgpNetwork6MaskLen
  - alaBgpNetwork6LocalPref
**ipv6 bgp network metric**

Configures the Multi-Exit Discriminator (MED) attribute value for an network generated by the `ipv6 bgp network` command. This value is sent from routers of one AS to another to indicate the path that the remote AS can use to send data to the local AS.

`ipv6 bgp network ipv6_address/prefix_length [metric num]`

### Syntax Definitions

- **ipv6_address**
  The 128-bit IPv6 address.

- **/prefix_length**
  The number of bits that are significant in the IPv6 address (mask) (3..128).

- **num**
  The MED attribute value. The valid range is 0–4294967295.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The IPv6 BGP route created with the `ipv6 bgp network` command should exist before the `metric` attribute is defined for the same route.

### Examples

```
-> ipv6 bgp network 2001::1/64 metric 20
```

### Release History

Release 7.1.1; command was introduced.
# Related Commands

**ipv6 bgp network**
Advertises a locally reachable IPv6 address as a IPv6 BGP network to other BGP peers.

**show ipv6 bgp network**
Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network

# MIB Objects

```markdown
alaBgpNetwork6Table
   alaBgpNetwork6Addr
   alaBgpNetwork6MaskLen
   alaBgpNetwork6Metric
```
ipv6 bgp network admin-state

Enables or disables a BGP network. The BGP status must be manually enabled after configuring all the BGP neighbor and network parameters.

`ipv6 bgp network ipv6_address/prefix_length [admin-state {enable | disable}]`

Syntax Definitions

- `ipv6_address`: The 128-bit IPv6 address.
- `/prefix_length`: The number of bits that are significant in the IPv6 address (mask) (3..128).
- `enable`: Enables the BGP network.
- `disable`: Disables the BGP network.

Defaults

By default, the BGP network is disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The IPv6 BGP route created with the `ipv6 bgp network` command should exist before the `status` attribute is defined.

Examples

```
-> ipv6 bgp network 2001::1/64 admin-state enable
```

Release History

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 bgp network* Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

**MIB Objects**

alaBgpNetwork6Table
- alaBgpNetwork6Addr
- alaBgpNetwork6MaskLen
- alaBgpNetwork6RowStatus
**show ipv6 bgp network**

Displays the status of all the IPv6 BGP networks or a specific IPv6 BGP network.

```
show ipv6 bgp network [ipv6_address/prefix_length]
```

### Syntax Definitions

- `<ipv6_address>`: The 128-bit IPv6 address.
- `<prefix_length>`: The number of bits that are significant in the IPv6 address (mask) (3..128).

### Defaults

By default, all IPv6 BGP networks and their status will be displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `<ipv6_address>/prefix_length` parameter to display the status of a specific IPv6 BGP network.

### Examples

```
show ipv6 bgp network
Network --------------------------------+-----------+----------
--------------------------------+-----------+----------
2525:500:600::/64                enabled     active

show ipv6 bgp network 2525:500:600::/64
Network address = 2525:500:600::/64,
Network admin state = enabled,
Network oper state = active,
Network metric = 0,
Network local preference = 0,
Network community string = <none>
```
## Output Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network or Network address</strong></td>
<td>The IPv6 address configured for this local BGP network. This value is configured through the <code>ipv6 bgp network</code> command.</td>
</tr>
<tr>
<td><strong>Admin state or Network admin state</strong></td>
<td>Indicates whether this local BGP network is administratively enabled or disabled. This value is configured through the <code>ipv6 bgp network admin-state</code> command.</td>
</tr>
<tr>
<td><strong>Oper state or Network oper state</strong></td>
<td>Indicates whether this BGP local network is operationally active or inactive.</td>
</tr>
<tr>
<td><strong>Network metric</strong></td>
<td>The multi-exit discriminator (MED) value configured for this local BGP network. This value is configured through the <code>ipv6 bgp network metric</code> command.</td>
</tr>
<tr>
<td><strong>Network local preference</strong></td>
<td>The local preference value for this local BGP network. This value is configured through the <code>ipv6 bgp network local-preference</code> command.</td>
</tr>
<tr>
<td><strong>Network community string</strong></td>
<td>The community string value for this local BGP network. This value is configured through the <code>ipv6 bgp network community</code> command.</td>
</tr>
</tbody>
</table>

## Release History

Release 7.1.1; command was introduced.

## Related Commands

- **ipv6 bgp network** Advertises a locally reachable IPv6 address as an IPv6 BGP network to other BGP peers.

## MIB Objects

alaBgpNetwork6Table
- alaBgpNetwork6Addr
- alaBgpNetwork6MaskLen
- alaBgpNetwork6State
- alaBgpNetwork6Metric
- alaBgpNetwork6LocalPref
- alaBgpNetwork6Community
- alaBgpNetwork6RowStatus
**ipv6 bgp neighbor**

Creates or deletes a BGP peer relationship using IPv6 addresses.

```
ipv6 bgp neighbor ipv6_address
no ipv6 bgp neighbor ipv6_address
```

### Syntax Definitions

`ipv6_address` The 128-bit IPv6 address of the new BGP peer.

### Defaults

By default, no BGP peers are configured in the BGP network.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to delete a BGP peer.
- To establish a BGP session, the BGP peer should be reachable.
- You must manually enable a BGP peer after creating it. A BGP peer is enabled using the `ipv6 bgp neighbor admin-state` command.
- Once created, a BGP peer must be assigned an autonomous system number using the `ipv6 bgp neighbor remote-as` command.
- Use `update-source` keyword to configure the IPv6 interface when link-local address is used as neighbor address.

### Examples

```
-> ipv6 bgp neighbor 2001::1
-> no ipv6 bgp neighbor 2001::1
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **ipv6 bgp neighbor admin-state**  Enables or disables the BGP peer status.
- **ipv6 bgp neighbor remote-as**  Assigns an AS number to the BGP peer.

MIB Objects

- alaBgpPeer6Table
- alaBgpPeer6Addr
**ipv6 bgp neighbor ttl-security**

Configures the Generalized TTL Security Mechanism (GTSM) for the BGP peer. GTSM allows to set the maximum number of hops for the IP packets between the switch and the peer. If the maximum number of hops exceeds, the packet is dropped at the NI.

```
ipv6 bgp neighbor ipv6_address ttl-security num
ipv6 bgp neighbor ipv6_address no ttl-security
```

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address of the BGP peer.
- `num`: The maximum number of hops between the switch and the peer. The valid range for GTSM is 0 to 255.

**Defaults**

By default GTSM is disabled for communication with the peer.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- GTSM must be manually enabled on both peers in a connection.
- When GTSM is enabled, eBGP multihop must be disabled or vise-versa.
- Use the `no` form of this command to disable GTSM.

**Examples**

```bash
-> ipv6 bgp neighbor 2001::1 ttl-security 6
-> ipv6 bgp neighbor 2001::1 no ttl-security
```

**Release History**

Release 8.4.1; command was introduced.
Related Commands

`show ipv6 bgp neighbors` Displays the configured IPv6 BGP peers.

MIB Objects

`alaBgpPeer6Table`
`alaBgpPeer6Addr`
`alaBgpPeer6TTLSecurityHops`
**ipv6 bgp neighbor activate-ipv4**

Enables the advertisement of IPv4 unicast capability to the IPv6 BGP peer.

```
ipv6 bgp neighbor ipv6_address [activate-ipv4]
no ipv6 bgp neighbor ipv6_address [activate-ipv4]
```

### Syntax Definitions

- **ipv6_address**
  - The 128-bit IPv6 address of the new BGP peer.

- **activate-ipv4**
  - Enable the advertisement of IPv4 unicast capability to the IPv6 BGP peer.

### Defaults

By default, the command is enabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **no** form of this command to disable the advertisement of IPv4 unicast capability to IPv6 BGP peer.

### Examples

- `-> ipv6 bgp neighbor 2001::1 activate-ipv4`
- `-> no ipv6 bgp neighbor 2001::1 activate-ipv4`

### Release History

Release 7.3.4; command was introduced.
**Related Commands**

`ipv6 bgp neighbor`  
Creates or deletes a BGP peer relationship using IPv6 addresses.

**MIB Objects**

alaBgpPeer6Table

  - alaBgpPeer6Addr
  - alaBgpPeer6ActivateIpv4
**ipv6 bgp neighbor activate-ipv6**

Enables the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

```
ipv6 bgp neighbor ipv6_address [activate-ipv6]
no ipv6 bgp neighbor ipv6_address [activate-ipv6]
```

### Syntax Definitions

`ipv6_address`  
The 128-bit IPv6 address.

### Defaults

This command is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `no` form of this command to disable the exchange of IPv6 unicast routes between BGP peer routers identified by their IPv6 addresses.

### Examples

```
-> ipv6 bgp neighbor 1.0.0.1 activate-ipv6
-> no ipv6 bgp neighbor 1.0.0.1 activate-ipv6
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show ipv6 bgp neighbors` Displays the configured IPv6 BGP peers.

### MIB Objects

- `alaBgpPeer6Table`  
- `alaBgpPeer6Addr`  
- `alaBgpPeer6ActivateIpv6`
**ipv6 bgp neighbor ipv6-nexthop**

Configures the IPv6 next hop addresses for IPv6 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

`ipv6 bgp neighbor ipv6_address [ipv6-nexthop ipv6_address]`

### Syntax Definitions

- `ipv6_address`: The 128-bit IPv6 address of the next hop router.

### Defaults

By default, the IPv6 next hop address is set to all zeros.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- To reset the IPv6 next hop value, enter an all-zero address.
- For internal BGP (IBGP) peers, the IPv6 next hop is used only if the peer `next-hop-self` option is configured.
- For external BGP (EBGP) peers, the IPv6 next hop is used for all the advertised IPv6 routes.
- For BGP peers configured with their link-local addresses, the configured IPv6 next hop is used while advertising IPv6 prefixes.

### Examples

- `-> ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24`
- `-> no ipv6 bgp neighbor 2001::1 ipv6-nexthop fe80::/24`

### Release History

Release 7.1.1; command was introduced.
Related Commands

show ipv6 bgp neighbors  Displays the configured IPv6 BGP peers.

MIB Objects

alaBgpPeer6Table
    alaBgpPeer6Addr
    alaBgpPeerIpv6NextHop
ipv6 bgp neighbor admin-state

Enables or disables the BGP peer status. These peers are identified by their IPv6 addresses.

ipv6 bgp neighbor ipv6_address [admin-state {enable | disable}]

Syntax Definitions

ipv6_address            The 128-bit IPv6 address of the new BGP peer.
enable                  Enables the BGP peer.
disable                 Disables the BGP peer.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- You should first create a BGP peer and assign it an IPv6 address using the ipv6 bgp neighbor command before enabling the peer.
- You should configure all the BGP peer related commands before enabling a BGP peer. Once you have enabled the peer, it will begin sending BGP connection and route advertisement messages.

Examples

-> ipv6 bgp neighbor 2001::1 admin-state enable
-> ipv6 bgp neighbor 2001::1 admin-state disable

Release History

Release 7.1.1; command was introduced.
**Related Commands**

`show ipv6 bgp neighbors`  Displays the configured IPv6 BGP peers.

**MIB Objects**

`alaBgpPeer6Table`  
- `alaBgpPeer6Addr`
- `alaBgpPeer6RowStatus`
ipv6 bgp neighbor clear

Restarts the IPv6 BGP peer. The peer will be unavailable during this restart.

ipv6 bgp neighbor ipv6_address clear

**Syntax Definitions**

*ipv6_address* The 128-bit IPv6 address of the neighbor.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command whenever changes occur to BGP-related access lists, weights, distribution lists, timer specifications, or administrative distance.
- Many peer commands restart the peer as soon as they are configured. The following commands restart the BGP peer for which they are configured:
  - ipv6 bgp neighbor remote-as
  - ipv6 bgp neighbor md5 key
  - ipv6 bgp neighbor passive
  - ipv6 bgp neighbor ebgp-multihop
  - ipv6 bgp neighbor maximum-prefix
  - ipv6 bgp neighbor update-source
  - ipv6 bgp neighbor next-hop-self
  - ipv6 bgp neighbor soft-reconfiguration
  - ipv6 bgp neighbor route-reflector-client
  - ip bgp confederation neighbor6
  - ipv6 bgp neighbor remove-private-as
  - ipv6 bgp neighbor update-source-address
- You do not need to issue the *ipv6 bgp neighbor clear* command after issuing any of the above commands.
**Examples**

-> ipv6 bgp neighbor 2001::1 clear

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

**ipv6 bgp neighbor auto-restart**

Automatically attempts to restart a BGP peer session after a session terminates.

**MIB Objects**

alaBgpPeer6Table

- alaBgpPeer6Restart
**ipv6 bgp neighbor auto-restart**

Enables or disables BGP peer automatic restart. When enabled, this IPv6 peer will automatically attempt to restart a session with another peer after a session with that peer terminates. When disabled, this peer will not try to re-establish a session with another peer after the session terminates; in such a case, the other peer will have to restart the session for the two peers to resume communication.

**ipv6 bgp neighbor ipv6_address auto-restart**

---

**Syntax Definitions**

*ipv6_address* The 128-bit IPv6 address of the neighbor.

**Defaults**

This command is enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable automatic peer restart.

- After a session with another peer terminates, the local BGP speaker will wait 60 seconds before attempting to restart the session. If the session does not start on the first attempt a second attempt will be made after another 120 seconds (60x2). On each unsuccessful session attempt, the previous delay between restarts is multiplied by 2, up to a maximum delay of 240 seconds. An exception to this rule occurs when the peer session terminates on receipt of a NOTIFY message with 'unsupported option' code or 'unsupported capability' code; in these cases the delay between restart attempts will begin at 1 second and multiply by 2 after each unsuccessful restart attempt (up to a maximum of 240 second delay).

- Disabling this option can be helpful in cases where other peers are prone to frequent flapping or sending many NOTIFY messages. By not restarting sessions with unstable neighbors, the local BGP speaker forces those unstable neighbors to re-initialize the connection.

**Examples**

-> ipv6 bgp neighbor 2001::1 auto-restart
-> no ipv6 bgp neighbor 2001::1 auto-restart

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- `ipv6 bgp neighbor` Creates or deletes a BGP peer relationship using IPv6 addresses.
- `ipv6 bgp neighbor admin-state` Enables or disables the BGP peer status.

MIB Objects

- `alaBgpPeer6Table`  
- `alaBgpPeer6AutoRestart`
**ipv6 bgp neighbor remote-as**

Assigns an AS number to the BGP peer.

```
ipv6 bgp neighbor ipv6_address [remote-as value]
```

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address of the BGP peer.
- `value`: Autonomous system number in the asplain, asdot+, or asdot formats.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A BGP peer created with the `ipv6 bgp neighbor` command cannot be enabled until it is assigned an autonomous system number. If the AS number assigned to the peer matches the AS number of the local BGP speaker (assigned using the `ip bgp autonomous-system` command), the peer is considered internal to the local autonomous system. Otherwise, the peer is considered external to the local BGP speaker’s AS.

- The BGP peer is restarted after issuing this command.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 remote-as 100
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; modified the command.
**Related Commands**

`ip bgp autonomous-system`  Sets the AS for the local BGP speaker.

**MIB Objects**

`alaBgpPeer6Table`
- `alaBgpPeer6Addr`
- `alaBgpPeer6AS`
ipv6 bgp neighbor timers

Configures the KEEPALIVE message interval and hold time interval (in seconds) with regards to the specified BGP peer.

**ipv6 bgp neighbor ipv6_address [timers num num]**

### Syntax Definitions

- **ipv6_address**: The 128-bit IPv6 address for the BGP peer.
- **num**: The KEEPALIVE message interval in seconds.
- **num**: The hold time interval in seconds.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num (keepalive)</td>
<td>30 seconds</td>
</tr>
<tr>
<td>num (holdtime)</td>
<td>90 seconds</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- KEEPALIVE messages do not contain route updates or indicate a change in the status of the BGP peer; they indicate to the receiving BGP peer that the connection is still live and the peer is reachable.

- By default, the KEEPALIVE interval of 30 seconds is one-third the default hold time interval of 90 seconds. The KEEPALIVE interval can never be more than one-third the value of the hold time interval. When the hold time interval is reached without receiving KEEPALIVE or other updates messages, the peer is considered dead.

- Setting the KEEPALIVE value to zero means no KEEPALIVE messages will be sent.

- Once a connection is established with a peer and a time period of the length specified in this command transpires with no messages from the remote peer, then the connection with that remote peer will be considered dead.

- The hold timer is used during the connection setup process and for on-going connection maintenance with BGP peers. If the peer does not receive a KEEPALIVE, UPDATE, or NOTIFICATION message within this time period, then the BGP connection will be closed.

- Both the KEEPALIVE and hold time interval should be set at the same time.
• Using this command without the variables resets the variables to their default value.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 timers 80 240
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`ipv6 bgp neighbor conn-retry-interval` The interval, in seconds, between BGP retries to set up a connection with another peer through the transport protocol.

**MIB Objects**

`alaBgpPeer6Table`
  `alaBgpPeer6Addr`
  `alaBgpPeer6HoldTime`
  `alaBgpPeer6KeepAlive`
ipv6 bgp neighbor maximum-prefix

Configures the maximum number of prefixes, or paths, the local router can receive from a BGP peer in UPDATE messages.

ipv6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]
no ipv6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]

Syntax Definitions

ipv6_address
   The 128-bit IPv6 address for the BGP peer.

num
   The number of prefixes. The valid range is 0–4294967295.

Defaults

+-----------------+------------------+
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>5000</td>
</tr>
</tbody>
</table>

By default, warning-only is enabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When the number of prefixes sent by the BGP peer reaches the maximum limit, the peer is restarted.
- You can use BGP logging to receive a warning when the number of prefixes received from the peer reaches 80 percent of the value you configure in this command.
- If the warning-only prefix is used, the operator will be warned when the peer exceeds 80 percent of the configured number of maximum prefixes.
- The BGP peer is restarted after issuing this command.

Examples

- ipv6 bgp neighbor 2001::2 maximum-prefix 1000 warning-only
- no ipv6 bgp neighbor 2001::2 maximum-prefix 1000

Release History

Release 7.1.1; command was introduced.
Related Commands

show ipv6 bgp neighbors  Displays the configured IPv6 BGP peers.

MIB Objects

alaBgpPeer6Table
  alaBgpPeer6Addr
  alaBgpPeer6MaxPrefix
  alaBgpPeer6MaxPrefixWarnOnly
**ipv6 bgp neighbor next-hop-self**

Configures router to advertise its peering address as the next hop address for the specified neighbor.

```plaintext
ipv6 bgp neighbor ipv6_address [next-hop-self]
o ipv6 bgp neighbor ipv6_address [next-hop-self]
```

**Syntax Definitions**

`ipv6_address` The 128-bit IPv6 address for the BGP peer.

**Defaults**

By default, the `next-hop-self` parameter of BGP updates is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the `next-hop-self` parameter.

- In meshed networks, the BGP peer may not have direct connections to other peers. When such a peer receives route updates from these distant peers (through other peers), it may treat the remote peer as if it were the next hop in the routing path. Packet forwarding will not work in such a case because no direct connection exists. This command allows the peer to deem itself the next hop on the routing path so that the two non-connected peers can route packets. This peer would have a direct connection to both peers that want to exchange packets.

- The BGP peer is restarted after issuing this command.

**Examples**

```plaintext
-> ipv6 bgp neighbor 2001::2 next-hop-self
-> no ipv6 bgp neighbor 2001::2 next-hop-self
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 bgp neighbors* Displays the configured IPv6 BGP peers.

**MIB Objects**

`alaBgpPeer6Table`
- `alaBgpPeer6Addr`
- `alaBgpPeer6NextHopSelf`
**ipv6 bgp neighbor conn-retry-interval**

The interval, in seconds, between BGP retries to set up a connection with another peer through the transport protocol. In the connect state, BGP tries to set up a connection with a remote peer. If the connection fails, then the connection retry interval starts. Once this interval elapses, BGP retries setting up the connection.

```
ipv6 bgp neighbor ipv6_address [conn-retry-interval num]
```

### Syntax Definitions

- `ipv6_address`: The 128-bit IPv6 address for the BGP neighbor.
- `num`: The time interval (in seconds) between retries. The valid range is 0–65535.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>120</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The connection retry time interval starts when a connection to a peer is lost.
- Using this command without the `num` variable resets the variable to its default value.

### Examples

```
-> ipv6 bgp neighbor 2001::2 conn-retry-interval 60
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

`show ipv6 bgp neighbors`  Displays the configured IPv6 BGP peers.

MIB Objects

`alaBgpPeer6Table`
- `alaBgpPeer6Addr`
- `alaBgpPeer6ConnRetryInterval`
**ipv6 bgp neighbor default-originate**

Enables or disables the BGP local speaker to advertise a default route to the peer.

```
ipv6 bgp neighbor ipv6_address [default-originate]
```

```
no ipv6 bgp neighbor ipv6_address [default-originate]
```

**Syntax Definitions**

`ipv6_address`  
The 128-bit IPv6 address for the neighbor.

**Defaults**

This `default-originate` parameter is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the BGP peer default origination.
- When this command is enabled, the local BGP speaker advertises the default route to the peer. Such a default route overrides any learned default (propagation) and outbound policy. The default route `::/0` does not need to exist on the local router.
- If the peer is capable of exchanging IP as well as IPv6 prefixes, the default route for both IP and IPv6 is advertised.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 default-originate
-> no ipv6 bgp neighbor 2001::1 default-originate
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`show ipv6 bgp neighbors`  
Displays the configured IPv6 BGP peers.

**MIB Objects**

`alaBgpPeer6Table`  
`alaBgpPeer6Addr`
ipv6 bgp neighbor default-originate
**ipv6 bgp neighbor update-source**

Configures the local IPv6 interface from which a BGP peer will be connected. This local IPv6 interface can be configured for internal and external BGP peers.

`ipv6 bgp neighbor ipv6_address [update-source interface_name]`

`no ipv6 bgp neighbor ipv6_address [update-source interface_name]`

---

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address for the BGP peer.
- `interface_name`: The name of the local IPv6 interface that provides the TCP connection for this BGP peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The BGP peer is restarted after issuing this command.
- If a BGP peer is configured with its link-local address, use the `update-source` parameter to specify the name of the IPv6 interface from which this peer is reachable. This is required to establish a BGP peering session.

**Examples**

- `-> ipv6 bgp neighbor 2004::1 update-source bgp_ipv6`
- `-> no ipv6 bgp neighbor 2004::1 update-source bgp_ipv6`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **show ipv6 bgp neighbors** Displays the configured IPv6 BGP peers.
- **ipv6 interface** Configures an IPv6 interface on a VLAN or IPv6 tunnel.

**MIB Objects**

- **alaBgpPeer6Table**
  - **alaBgpPeer6Addr**
  - **alaBgpPeer6LocalIntfName**
**ipv6 bgp neighbor ipv4-nexthop**

Configures the IP4 next hop addresses for IP4 prefixes advertised between BGP peers. These BGP peers are identified by their IPv6 addresses.

```
ipv6 bgp neighbor ipv6_address [ipv4-nexthop ip_address]
```

### Syntax Definitions

- `ipv6_address` The 128-bit IPv6 address for the BGP peer.
- `ip_address` The 32-bit IP address of the next hop.

### Defaults

By default, the IPv4 next hop value is set to all zeros.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To reset the IPv4 next hop value, enter an all-zero address.

### Examples

```
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 172.22.2.115
-> ipv6 bgp neighbor 2004::1 ipv4-nexthop 0.0.0.0
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show ipv6 bgp neighbors`. Displays the configured IPv6 BGP peers.

### MIB Objects

- `alaBgpPeer6Table`
  - `alaBgpPeer6Addr`
  - `alaBgpPeer6Ipv4NextHop`
**ipv6 bgp neighbor advertisement-interval**

Configures the time interval for updates between external IPv6 BGP peers.


```
ipv6 bgp neighbor ipv6_address advertisement-interval value
```

### Syntax Definitions

- `ipv6_address`: The 128-bit IPv6 address for the neighbor.
- `value`: An advertisement time interval in seconds. The valid range is 0–65535.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>30</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Internal peers sharing the same AS as the local BGP speaker (configured in the `ip bgp autonomous-system` command) use the global route advertisement update interval. This command sets the interval this peer uses to send BGP UPDATE messages to external IPv6 BGP peers.

### Examples

- `ipv6 bgp neighbor 2001::1 advertisement-interval 60`

### Release History

Release 7.3.4; command was introduced.
Related Commands

show ipv6 bgp neighbors Display the configured IPv6 BGP peers.

MIB Objects

alaBgpPeer6Table
  alaBgpPeer6Addr
  alaBgpPeer6MinRouteAdvertisementInterval
**ipv6 bgp neighbor description**

Configures the IPv6 BGP Peer name.

*ipv6 bgp neighbor ipv6_address description string*

**Syntax Definitions**

- **ipv6_address**: The 128-bit IPv6 address for the neighbor.
- **string**: Peer name (1 - 20 characters).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>peer (ipv6_address)</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The peer name is a text identifier that, by default, follows the format "peer(ipv6-address)" where ipv6-address is the IPv6 address of the BGP peer. For example, the default name of an IPv6 BGP peer at address 2001::1 would be “peer(2001::1)”.
- A peer name with embedded spaces must be enclosed in quotation marks.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 description "peer6 for building 3"
```

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- **ipv6 bgp neighbor**: Creates or deletes a BGP peer relationship using IPv6 addresses.

**MIB Objects**

- **alaBgpPeer6Table**
- **alaBgpPeer6Addr**
ipv6 bgp neighbor description

alaBgpPeer6Name
**ipv6 bgp neighbor ebgp-multihop**

Allows external IPv6 BGP peers to communicate with each other even when they are not directly connected. The absence of communication between disconnected peers can occur when a router that is not running BGP sits between two BGP speakers; in such a scenario the BGP speakers are multiple hops from each other. By enabling this command, you allow the IPv6 BGP peers to speak to each other despite the non-BGP router that sits between them.

```
ipv6 bgp neighbor ipv6_address ebgp-multihop [ttl]
```

```
no ipv6 bgp neighbor ipv6_address ebgp-multihop
```

**Syntax Definitions**

- `ipv6_address` - The 128-bit IPv6 address of the BGP peer.
- `ttl` - The Time to Live for the multi-hop connection, in seconds. The range is 1 to 255.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ttl</code></td>
<td>255</td>
</tr>
</tbody>
</table>

This command is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable multi-hop connections.
- By default an external IPv6 BGP peer is on a directly connected subnet. This command allows you to configure an external IPv6 BGP peer that is not directly connected and may be multiple hops away. It should be used with caution and only with the guidance of qualified technical support.
- The BGP peer is restarted after issuing this command.
- When eBGP multihop is enabled, GTSM must be disabled or vice-versa.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 ebgp-multihop
-> ipv6 bgp neighbor 2001::1 ebgp-multihop 50
```
-> no ipv6 bgp neighbor 2001::1 ebgp-multihop

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

**ipv6 bgp neighbor**  
Creates or deletes a BGP peer relationship using IPv6 addresses.

**ipv6 bgp neighbor next-hop-self**  
Configures router to advertise its peering address as the next hop address for the specified neighbor.

**MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaBgpPeer6Table</td>
<td></td>
</tr>
<tr>
<td>alaBgpPeer6Addr</td>
<td></td>
</tr>
<tr>
<td>alaBgpPeer6MultiHop</td>
<td></td>
</tr>
</tbody>
</table>
**ipv6 bgp neighbor update-source-address**

Configures the local IPv6 address from which a BGP peer will be connected if the peer is configured with its link-local address. This local IPv6 address can be configured for internal and external BGP peers.

```
ipv6 bgp neighbor ipv6_address update-source-address ipv6_address
no ipv6 bgp neighbor ipv6_address update-source-address ipv6_address
```

**Syntax Definitions**

`ipv6_address`  
The 128-bit IPv6 address of the BGP peer.

**Defaults**

By default, the update-source-address value is set to all zeros.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The BGP peer is restarted after issuing this command.
- The default is restored by using the `no` form of the command or by entering an all-zero address.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 update-source-address 2401::1
-> no ipv6 bgp neighbor 2001::1 update-source-address
```

**Release History**

Release 7.3.4; command was introduced.
**Related Commands**

- **ipv6 bgp neighbor update-source**  
  Configures the local IPv6 interface from which a BGP peer will be connected.

- **show ipv6 bgp neighbors**  
  Displays the configured IPv6 BGP peers.

**MIB Objects**

- `alaBgpPeer6Table`
- `alaBgPeer6LocalAddr`
ipv6 bgp neighbor passive

Configures the local IPv6 BGP speaker to wait for this IPv6 BGP peer to establish a connection. When enabled, the local BGP speaker will not initiate a peer session with this peer; in this sense, the BGP speaker is “passive.” When disabled, the local BGP speaker will attempt to set up a session with this peer.

ipv6 bgp neighbor ipv6_address passive

no ipv6 bgp neighbor ipv6_address passive

Syntax Definitions

ipv6_address

The 128-bit IPv6 address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable passive peer behavior.
- By default, BGP will initiate a session to a peer once the peer is configured, has an AS number, and is enabled. You can use this command to configure the local BGP speaker as passive and an outbound session will not be initiated to this peer. For such peers, BGP will always wait passively for the inbound session attempt.
- The BGP peer is restarted after issuing this command.

Examples

-> ipv6 bgp neighbor 2001::1 passive
-> no ipv6 bgp neighbor 2001::1 passive

Release History

Release 7.3.4; command was introduced.
**Related Commands**

*ipv6 bgp neighbor*  
Creates or deletes a BGP peer relationship using IPv6 addresses.

**MIB Objects**

alaBgpPeer6Table

*alaBgpPeer6Addr*
*alaBgpPeer6Passive*
ipv6 bgp neighbor remove-private-as

Enables or disables the stripping of private autonomous system numbers from the AS path of routes destined to this peer.

ipv6 bgp neighbor ipv6_address remove-private-as

no ipv6 bgp neighbor ipv6_address remove-private-as

### Syntax Definitions

*ipv6_address*  
The 128-bit IPv6 address of the BGP peer.

### Defaults

This command is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

|                | 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 V72/C32 | 6900 X48C6/T48C6/ \n|----------------|------|------|------|-------|------|-------|------|------|-----------------| X48C4E/V48C8/ \n|                | No   | No   | No   | No    | Yes  | Yes   | Yes  | Yes  | C32E/T24C2/     \n|                |      |      |      |       |      |       |      |      | X24C2           |

### Usage Guidelines

- Use the *no* form of this command to disable stripping of private AS numbers.
- By default, all AS numbers in the AS path are passed to peers. Enabling this command strips any private AS numbers in the AS path before sending updates to this peer. AS numbers in the range 64512 to 65535 are considered private ASs; they are intended for internal use within an organization (such as an enterprise network), but they are not intended for use on public networks (such as the Internet).
- This command has no effect if you are not using ASs in the range 64512 to 65535.
- The BGP peer is restarted after issuing this command.

### Examples

-> ipv6 bgp neighbor 2001::1 remove-private-as
-> no ipv6 bgp neighbor 2001::1 remove-private-as

### Release History

Release 7.3.4; command was introduced.
Related Commands

**ipv6 bgp neighbor remote-as** Assigns an AS number to the BGP peer.

**MIB Objects**

`alaBgpPeer6Table`  
  `alaBgpPeer6Addr`  
  `alaBgpPeer6RemovePrivateAs`
ipv6 bgp neighbor soft-reconfiguration

Enables or disables IPv6 BGP peer soft reconfiguration. Soft reconfiguration increases the stability of the peer by allowing you to reconfigure attributes that require peer resets without halting the TCP connection with other peers.

ipv6 bgp neighbor ipv6_address soft-reconfiguration

no ipv6 bgp neighbor ipv6_address soft-reconfiguration

Syntax Definitions

ipv6_address The 128-bit IPv6 address of the BGP peer.

Default

This command is enabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable this feature.
- This feature stores routes and other configuration information in local memory. When you make configuration changes that require a peer reset, the routing cache is not cleared and connections with other peers are not interrupted.
- If a peer is not route-refresh capable, by default, BGP stores all paths from peers, even those that are policy rejected, in anticipation of policy changes in the future. Storing these paths consumes memory. You can use this command to disable the storing of these paths, or soft reconfiguration. However, if soft reconfiguration is disabled and the peer is not route-refresh capable and the inbound policy changes, the peer will have to be restarted using the ipv6 bgp neighbor clear command.
- If the peer is route-refresh capable and soft reconfiguration is disabled, inbound policy changes are still supported without re-starting the peer.

Examples

- ipv6 bgp neighbor 2001::1 soft-reconfiguration
- no ipv6 bgp neighbor 2001::1 soft-reconfiguration
**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `ipv6 bgp neighbor clear`  
  Restarts the IPv6 BGP peer.

- `ipv6 bgp neighbor clear soft`  
  Invokes an inbound or outbound policy reconfiguration for an IPv6 BGP peer.

**MIB Objects**

- `alaBgpPeer6Table`
  - `alaBgpPeer6Addr`
  - `alaBgpPeer6SoftReconfig`
**ipv6 bgp neighbor stats-clear**

Clears the statistics for a peer.

**ipv6 bgp neighbor ipv6_address stats-clear**

---

**Syntax Definitions**

- *ipv6_address* The 128-bit IPv6 address of the BGP peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>V72/C32</th>
<th>V8C6/T48C6</th>
<th>V48C8/C32E/T24C2</th>
<th>X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command clears the statistical variables for a peer so they can accumulate from a known point.

- The cleared statistics include the total messages sent and received from this peer, the total UPDATE messages sent and received from this peer, the total NOTIFY messages sent and received from this peer, and the total peer state transition messages sent and received from this peer. These statistics can be displayed through **show ipv6 bgp neighbors statistics**.

**Examples**

```
-> ipv6 bgp neighbor 2001::2 stats-clear
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show ipv6 bgp neighbors statistics** Displays the neighbor statistics of the configured IPv6 BGP peers.

**MIB Objects**

- `alaBgpPeer6Table`  
  - `alaBgpPeer6Addr`  
  - `alaBgpPeer6ClearCounter`
ip bgp confederation neighbor6

Configures this IPv6 BGP peer as a member of the same confederation as the local BGP speaker.

ip bgp confederation neighbor6 ipv6_address

no ip bgp confederation neighbor6 ipv6_address

Syntax Definitions

ipv6_address

The 128-bit IPv6 address of the BGP peer.

Defaults

This command is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>6900 X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable this feature.
- You must first assign a confederation number to the local BGP speaker before assigning peers to the confederation. Use the ip bgp confederation identifier command to assign a confederation number to the local BGP speaker.

Examples

-> ip bgp confederation neighbor6 2001::1
-> no ip bgp confederation neighbor6 2001::1

Release History

Release 7.3.4; command was introduced.
Related Commands

**ip bgp confederation identifier** Sets a confederation identification value for the local BGP speaker (this router).

MIB Objects

alaBgpPeer6Table
- alaBgpPeerAddr
- alaBgPeer6ConfedStatus
**ipv6 bgp neighbor in-aspathlist**

Assigns an inbound AS path list filter to a BGP peer.

```
ipv6 bgp neighbor ipv6_address in-aspathlist {string | none}
```

### Syntax Definitions

- **ipv6_address**
  - The 128-bit IPv6 address of the BGP peer.
- **string**
  - Inbound AS path list (0 to 70 characters). This name is case sensitive.
- **none**
  - Removes this AS path list from the peer.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The AS path list name (*InboundASPath* in the example below) is created using the `ip bgp policy aspath-list` command. Any inbound routes from the BGP peer must match this AS path filter before being accepted or passed to an inbound policy.
- Use **none** to deassign an AS path filter list from this peer.

### Examples

- `-> ipv6 bgp neighbor 2001::1 in-aspathlist InBoundASpath`
- `-> ipv6 bgp neighbor 2001::1 in-aspathlist none`

### Release History

Release 7.3.4; command introduced.
Related Commands

*ip bgp policy aspath-list*  Creates or removes an AS path list.

MIB Objects

*alaBgpPeer6Table*

  *alaBgpPeer6AspathListIn*
**ipv6 bgp neighbor in-communitylist**

Assigns an inbound community list filter to a BGP peer.

```
ipv6 bgp neighbor ipv6_address in-communitylist {string | none}
```

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address of the BGP peer.
- `string`: Input community list (0 to 70 characters). This name is case sensitive.
- `none`: Removes this community list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The community filter list name (`InboundCommlist` in the example below) is created using the `ip bgp policy community-list` command. Any inbound routes from the BGP peer must match this community filter before being accepted or passed to inbound policy.

- Use `none` to deassign an input community filter list from this peer.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 in-communitylist InboundCommlist
-> ipv6 bgp neighbor 2001::1 in-communitylist none
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

**ip bgp policy community-list**  Creates or deletes a community list.

MIB Objects

alaBgpPeer6Table
  alaBgpPeer6CommunityListIn
**ipv6 bgp neighbor in-prefixlist**

Assigns an inbound prefix filter list to a BGP peer.

```
ipv6 bgp neighbor ipv6_address in-prefixlist {string | none}
```

**Syntax Definitions**

- `ipv6_address` The 128-bit IPv6 address of the BGP peer.
- `string` Input prefix filter list (0 to 70 characters). This name is case sensitive.
- `none` Removes the prefix list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The prefix list name (**InboundPrefix** in the example below) is created using the `ip bgp policy prefix-list` command. Any inbound IPv4 routes from the BGP peer must match this prefix filter before being accepted or passed to inbound policy.
- Use `none` to deassign an input prefix filter list from this peer.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 in-prefixlist InboundPrefix
-> ipv6 bgp neighbor 2001::1 in-prefixlist none
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

`ip bgp policy prefix-list` Creates or deletes a prefix match list.

MIB Objects

`alaBgpPeer6Table` `alaBgpPeer6PrefixListIn`
**ipv6 bgp neighbor in-prefix6list**

Assigns an inbound prefix6 list to a BGP peer.

```
ipv6 bgp neighbor ipv6_address in-prefix6list {string | none}
```

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address of the BGP peer.
- `string`: Input prefix6 filter list (0 to 70 characters). This name is case sensitive.
- `none`: Removes the prefix6 list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The prefix6 list name (**InboundPrefix6** in the example below) is created using the `ip bgp policy prefix6-list` command. Any inbound IPv6 routes from the BGP peer must match this prefix6 filter before being accepted or passed to inbound policy.
- To deassign an input prefix6 filter list, use this command to assign a value of “none.”

**Examples**

```
-> ipv6 bgp neighbor 2001::2 in-prefix6list InboundPrefix6
-> ipv6 bgp neighbor 2001::2 in-prefix6list none
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

ip bgp policy prefix6-list

Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

MIB Objects

alaBgpPeer6Table
  alaBgpPeer6Prefix6ListIn
ipv6 bgp neighbor out-aspathlist

Assigns an outbound AS path filter list to a BGP peer.

**ipv6 bgp neighbor ipv6_address out-aspathlist {string | none}**

---

**Syntax Definitions**

*ipv6_address*  
The 128-bit IPv6 address of the BGP peer.

*string*  
Outbound AS path list (0 - 70 characters).

*none*  
Removes the AS path list from the peer.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The AS path list name (*OutboundASpath* in the example below) is created using the **ip bgp policy aspath-list** command. Any outbound routes from the BGP peer must match this AS path filter, or policy, before being advertised or passed to outbound policy.

- Use **none** to deassign an output AS path filter list from this peer.

---

**Examples**

- `-> ipv6 bgp neighbor 2001::1 out-aspathlist OutboundASPath`
- `-> ipv6 bgp neighbor 2001::1 out-aspathlist none`

---

**Release History**

Release 7.3.4; command was introduced.
**Related Commands**

`ip bgp policy aspath-list`  Creates or removes an AS path list.

**MIB Objects**

alaBgpPeer6Table

- alaBgpPeer6AspathListOut
**ipv6 bgp neighbor out-communitylist**

Assigns an outbound community filter list to a BGP peer.

```
ipv6 bgp neighbor ipv6_address out-communitylist {string | none}
```

### Syntax Definitions

- **ipv6_address**: The 128-bit IPv6 address of the BGP peer.
- **string**: Outbound AS path list (0 - 70 characters).
- **none**: Removes the community list from the peer.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The community filter list name (**OutboundCommlist** in the example below) is created using the `ip bgp policy community-list` command. Any outbound routes from the BGP peer must match this community filter before being advertised or passed to outbound policy.
- Use **none** to deassign an output community filter list from this peer.

### Examples

```
-> ipv6 bgp neighbor 2001::1 out-communitylist OutboundCommlist
-> ipv6 bgp neighbor 2001::1 out-communitylist none
```

### Release History

Release 7.3.4; command was introduced.
BGP Commands

ipv6 bgp neighbor out-communitylist

Related Commands

`ip bgp policy community-list` Creates or deletes a community list.

MIB Objects

`alaBgpPeer6Table`

`alaBgpPeer6CommunityListOut`
**ipv6 bgp neighbor out-prefixlist**

Assigns an outbound prefix filter list to a BGP peer.

`ipv6 bgp neighbor ipv6_address out-prefixlist {string | none}`

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address of the BGP peer.
- `string`: Outbound prefix filter list (0 - 70 characters).
- `none`: Removes the prefix filter list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The prefix list name (OutboundPrefix in the example below) is created using the `ip bgp policy prefix-list` command. Any outbound routes from the BGP peer must match this prefix filter before being advertised or passed to an outbound policy.
- Use `none` to deassign an output prefix filter list from this peer.

**Examples**

```
-> ipv6 bgp neighbor 2001::1 out-prefixlist OutboundPrefix
-> ipv6 bgp neighbor 2001::1 out-prefixlist none
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

ip bgp policy prefix-list Creates or deletes a prefix match list.

MIB Objects

alaBgpPeer6Table
   alaBgpPeer6PrefixListOut
**ipv6 bgp neighbor out-prefix6list**

Assigns an outbound prefix6 filter list to a BGP peer.

```
ipv6 bgp neighbor ipv6_address out-prefix6list \{string | none\}
```

**Syntax Definitions**

- `ipv6_address` The 128-bit IPv6 address of the BGP peer.
- `string` Outbound prefix6 filter list (0 - 70 characters).
- `none` Removes the prefix6 filter list from the peer.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The prefix6 list name (OutboundPrefix6 in the example below) is created using the `ip bgp policy prefix6-list` command. Any outbound IPv6 routes from the BGP peer must match this prefix6 filter before being advertised or passed to outbound policy.
- To deassign an output prefix6 filter list, use this command to assign a value of “none”.

**Examples**

```
-> ipv6 bgp neighbor 2001::2 out-prefix6list OutboundPrefix6
-> ipv6 bgp neighbor 2001::2 out-prefix6list none
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

**ip bgp policy prefix6-list**  
Configures a BGP prefix6-list policy for filtering IPv6 prefixes.

**MIB Objects**

alaBgpPeer6Table  
alaBgpPeer6Prefix6ListOut
**ipv6 bgp neighbor route-map**

Assigns a policy map to an IPv6 BGP peer.

```
ipv6 bgp neighbor ipv6_address route-map {string | none} {in | out}
no ipv6 bgp neighbor ipv6_address route-map {in | out}
```

### Syntax Definitions

- **ipv6_address**
  - The 128-bit IPv6 address of the peer.

- **string**
  - Policy map name (0 to 70 characters). This name is case sensitive.

- **none**
  - Deletes the route map if entered rather than a text string.

- **in**
  - Designates this route map policy as an inbound policy.

- **out**
  - Designates this route map policy as an outbound policy.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to deassign a policy map.
- The policy route map name (**InboundRoute** and **OutboundRoute** in the example below) is created using the `ip bgp policy route-map` command. Any routes from the BGP peer must match this route map filter before being accepted or passed to a policy.
- It is also possible to deassign a route map by entering `none` in place of a route map name.

### Examples

- `-> ipv6 bgp neighbor 2001::1 route-map InboundRoute in`
- `-> ipv6 bgp neighbor 2001::1 route-map OutboundRoute out`
- `-> ipv6 bgp neighbor 2001::1 route-map none in`
- `-> no ipv6 bgp neighbor 2001::1 route-map in`

### Release History

Release 7.3.4; command introduced.
Related Commands

`ip bgp policy route-map` Creates or deletes a policy route map.

MIB Objects

`alaBgpPeer6Table`

- `alaBgpPeer6RouteMapIn`
- `alaBgpPeer6RouteMapOut`
**ipv6 bgp neighbor clear soft**

Invokes an inbound or outbound policy reconfiguration for an IPv6 BGP peer.

```
ipv6 bgp neighbor ipv6_address clear soft {in | out}
```

### Syntax Definitions

- **ipv6_address**: The 128-bit IPv6 address for the BGP peer.
- **in**: Applies reconfiguration to the inbound policies.
- **out**: Applies reconfiguration to the outbound policies.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 bgp</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>neighbor</td>
<td>in</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>clear</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>soft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>{in</td>
<td>out}</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command reconfigures (or reapplies) all inbound or outbound policies to existing routes without restarting the peer session.
- This command is useful if policies have been changed.

### Examples

```
-> ipv6 bgp neighbor 2001::1 clear soft in
-> ipv6 bgp neighbor 2001::1 clear soft out
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **ipv6 bgp neighbor soft-reconfiguration**: Enables or disables IPv6 BGP peer soft reconfiguration.

### MIB Objects

- `alaBgpPeer6Table`
- `alaBgpPeer6ReconfigureInBound`
alaBgpPeer6ReconfigureOutBound
**ipv6 bgp neighbor route-reflector-client**

Configuration this IPv6 BGP peer as one of the clients to the local route reflector.

`ipv6 bgp neighbor ipv6_address route-reflector-client`

`no ipv6 bgp neighbor ipv6_address route-reflector-client`

### Syntax Definitions

`ipv6_address`  
The 128-bit IPv6 address for the BGP peer.

### Defaults

By default, the command is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to disable IPv6 BGP peer as a client to the local route reflector.
- The IPv6 BGP peers configured using this command become part of the client group. The remaining peers become the members of the non-client group for the local route reflector.
- When IPv6 BGP Peer is configured as route reflector client, all internal BGP speakers in an autonomous system need not be fully meshed. Instead, this route reflector takes the responsibility for passing internal BGP-learned routes to its peers.

### Examples

```plaintext
-> ipv6 bgp neighbor 2001::1 route-reflector-client
-> no ipv6 bgp neighbor 2001::1 route-reflector-client
```

### Release History

Release 7.3.4; command was introduced.
Related Commands

show ipv6 bgp neighbors  .Displays the configured IPv6 BGP peers.

MIB Objects
alaBgpPeer6Table
  alaBgpPeer6Addr
  alaBgpPeer6ClientStatus
**ipv6 bgp neighbor md5 key**

Configures an encrypted MD5 signature for TCP sessions with this IPv6 peer.

```
ipv6 bgp neighbor ipv6_address md5 key {string | none}
```

### Syntax Definitions

- **ipv6_address**: The 128-bit IPv6 address for the BGP peer.
- **string**: The MD5 public key. The maximum character length is 80.
- **none**: Remove the password and disable authentication.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The BGP peer is restarted after issuing this command.
- The password you specified in this command is encrypted before it appears in a saved snapshot file. However, if you view this command in a snapshot file or **boot.cfg** file, the command is displayed in a different syntax as given below:

```
ipv6 bgp neighbor ipv6_address md5 key-encrypt encrypted_string
```

**Note.** This MD5 password will not work, if this syntax is used to set it.

### Examples

- `-> ipv6 bgp neighbor 2001::1 md5 key openpeer2`
- `-> ipv6 bgp neighbor 2001::1 md5 key none`

### Release History

Release 7.3.4; command was introduced.
Related Commands

**ipv6 bgp neighbor**  Creates or deletes a BGP peer relationship using IPv6 addresses.

MIB Objects

alaBgpPeer6Table
  - alaBgpPeer6Addr
  - alaBgpPeer6MD5Key
**show ipv6 bgp neighbors**

Displays the configured IPv6 BGP peers.

**show ipv6 bgp neighbors [ipv6_address]**

### Syntax Definitions

- **ipv6_address**

  The 128-bit IPv6 address for the BGP neighbor.

### Defaults

By default, all the configured IPv6 BGP peers will be displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **ipv6_address** parameter to display the details of a specified IPv6 BGP peer.

### Examples

```bash
-> show ipv6 bgp neighbors
Legends: Nbr = Neighbor
         As = Autonomous System

Nbr address    As   Admin state Oper state  BGP Id   Up/Down      BFD Status
------------------------+----+-----------+-----------+--------+-----------+--------
2001:100:3:4::1          30   enabled     established 11.4.0.1 01h:42m:08s enabled
fe80::200:57ff:fe28:7e89 10   enabled     established 11.5.0.1 01h:40m:58s disabled
```

```bash
-> show ipv6 bgp neighbors 2001:100:3:4::1
Neighbor address = 2001:100:3:4::1,
Neighbor autonomous system = 30,
Neighbor Admin state = enabled,
Neighbor Oper state = established,
Neighbor passive status = disabled,
Neighbor name = peer(2101::51),
Neighbor local address = 2001:100:3:4::10,
Neighbor EBGP multiHop = disabled,
Neighbor next hop self = disabled,
Neighbor TTL security = 6,
Neighbor Route Refresh = enabled,
Neighbor Ipv4 unicast = enabled,
Neighbor Ipv4 multicast = disabled,
```
Neighbor type = internal,
Neighbor auto-restart = enabled,
Neighbor route-reflector-client = disabled,
Neighbor confederation status = disabled,
Neighbor remove private AS = disabled,
Neighbor default originate = disabled,
Neighbor maximum prefixes = 5000,
Neighbor max prefixes warning = enabled,
# of prefixes received = 10,
Neighbor MD5 key = <none>,
Neighbor local port = 49154,
Neighbor TCP window size = 32768,
Graceful Restart State = NotRestarting,
Advertised Restart Interval = 0s,
Forwarding State during restart = NotPreserved,
Activate IPv6 unicast = enabled,
Configured IPv4 NextHop Address = 0.0.0.0,
Configured IPv6 NextHop Address = ::,
Neighbor IPv6 unicast = advertised,
BFD Status = enabled,
Activate IPv4 unicast = enabled,
Activate check-first-AS = enabled

output definitions

<table>
<thead>
<tr>
<th>Nbr address or Neighbor address</th>
<th>The IPv6 address for this BGP peer. Assign this address through the ipv6 bgp neighbor command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>As or Neighbor autonomous system</td>
<td>The autonomous system to which this peer belongs. A peer’s AS number is assigned through the ipv6 bgp neighbor remote-as command.</td>
</tr>
<tr>
<td>Admin state or Neighbor Admin state</td>
<td>Indicates whether this peer has been enabled or disabled through the ipv6 bgp neighbor admin-state command.</td>
</tr>
<tr>
<td>Oper state or Neighbor Oper state</td>
<td>The current BGP state for this peer. Possible states are idle, connect, active, opensent, openconfirm, and established.</td>
</tr>
<tr>
<td>BGP Id</td>
<td>The unique BGP identifier of the peer.</td>
</tr>
<tr>
<td>Up/Down</td>
<td>The time since this peer has transitioned to its current UP or DOWN state. If the peer is currently Established, then this is the time that the peer has been UP. If the peer is currently Idle, then this is the time the peer has been DOWN.</td>
</tr>
<tr>
<td>Neighbor passive status</td>
<td>Indicates whether the local BGP speaker is “passive” (i.e., waiting for this peer to initiate a session).</td>
</tr>
<tr>
<td>Neighbor name</td>
<td>The name assigned to this peer.</td>
</tr>
<tr>
<td>Neighbor local address</td>
<td>The interface assigned to this peer. This value is configured through the ipv6 bgp neighbor update-source command.</td>
</tr>
<tr>
<td>Neighbor EBGP multiHop</td>
<td>Indicates whether BGP multi-hop support is enabled or disabled. This supports allows external BGP peers to communicate with each other even when they are not directly connected.</td>
</tr>
<tr>
<td>Neighbor next hop self</td>
<td>Indicates whether this peer is using next hop processing. This value is configured through the ipv6 bgp neighbor next-hop-self command.</td>
</tr>
<tr>
<td>Neighbor TTL security</td>
<td>Displays the number of hops between the switch and the peer. If the GTSM is disabled the value is displayed as none.</td>
</tr>
</tbody>
</table>
### Neighbor Route Refresh
Indicates whether this peer supports Route Refresh capability as defined in RFC 2918. This capability is an alternative to soft-reconfiguration that can save CPU and memory resources. It allows peers to dynamically request the re-advertisement of BGP routing tables. Since this router supports route refresh all BGP peers are automatically enabled for this capability.

### Neighbor Ipv4 unicast
Indicates whether this peer is multiprotocol IPv4 unicast capable.

### Neighbor Ipv4 multicast
Indicates whether this peer is multiprotocol IPv4 multicast capable.

### Neighbor type
Indicates whether this peer is internal or external to the AS.

### Neighbor auto-restart
Indicates whether peer auto-restart is enabled or disabled.

### Neighbor route-reflector-client
Indicates whether this peer is a client to the local route reflector, if configured.

### Neighbor confederation status
Indicates whether this peer is a member of a BGP confederation.

### Neighbor remove private AS
Indicates whether the stripping of private AS numbers (64512 to 65535) from AS paths is enabled or disabled.

### Neighbor default originate
Indicates whether peer default origination is enabled or disabled. When enabled, the local BGP speaker advertises the default route to the peer. This value is configured through the `ipv6 bgp neighbor default-originate` command.

### Neighbor maximum prefixes
The maximum number of prefixes the local router can receive in UPDATE from this peer. This value is configured through the `ipv6 bgp neighbor maximum-prefix` command.

### Neighbor max prefixes warning
Indicates whether a warning will be issued when this peer exceeds 80 percent of the maximum prefix value. This value is configured through the `ipv6 bgp neighbor update-source` command.

### # of prefixes received
Displays the total number of prefixes received by this neighbor.

### Neighbor MD5 key
When present, shows an encrypted version of the MD5 password. When not present, and MD5 password has not been configured.

### Neighbor local port
The TCP port used for the session with this peer.

### Neighbor TCP window size
The size of the TCP window for this BGP session. This value will always be 32768 as that is the maximum size of a BGP message.

### Graceful Restart State
Indicates the graceful restart state. This feature does not support IPv6 prefixes.

### Advertised Restart Interval
Indicates the restart interval in seconds.

### Forwarding State during restart
Indicates whether the peer has preserved the forwarding state during the graceful restart.

### Activate IPv6 unicast
Indicates whether or not IPv6 unicast advertisements are enabled. Options include `enabled` or `disabled`.

### Configured IPv4 NextHop Address
Specifies the IPv4 nexthop address. This is specified using the `ipv6 bgp neighbor ipv4-nexthop` command.

### Configured IPv6 NextHop Address
Specifies the IPv6 nexthop address. This is specified using the `ipv6 bgp neighbor ipv6-nexthop` command.

### Neighbor Ipv6 unicast
Indicates whether or not IPv6 unicast capability is advertised between the peers. Options include `enabled` or `disabled`.

### output definitions (continued)
output definitions (continued)

<table>
<thead>
<tr>
<th>BFD Status</th>
<th>Indicates whether BFD is enabled or disabled for this peer. The BFD status is configured through the <code>ipv6 bgp neighbor bfd-state</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate IPv4 unicast</td>
<td>Indicates whether or not IPv4 unicast capability is advertised between the peers. Options include enabled or disabled.</td>
</tr>
<tr>
<td>Activate check-first-AS</td>
<td>Displays the operational status of check for first AS in the AS_PATH list.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; ‘Activate IPv4 unicast’ output field added.
Release 8.4.1; ‘Neighbor TTL security’ output field added.
Release 8.7 R1; ‘Activate check-first-AS’ output field added.

Related Commands

- `ipv6 bgp neighbor` Creates or deletes a BGP peer relationship using IPv6 addresses
- `ipv6 bgp neighbor admin-state` Enables or disables the BGP peer status.
- `ipv6 bgp neighbor ttl-security` Configures the Generalized TTL Security Mechanism (GTSM) for the BGP peer.

MIB Objects

alaBgpPeer6Table
- alaBgpPeer6Addr
- alaBgpPeer6AS
- alaBgpPeer6Passive
- alaBgpPeer6Name
- alaBgpPeer6MultiHop
- alaBgpPeer6MaxPrefix
- alaBgpPeer6MaxPrefixWarnOnly
- alaBgpPeer6NextHopSelf
- alaBgpPeer6TTLSecurityHops
- alaBgpPeer6SoftReconfig
- alaBgpPeer6InSoftReset
- alaBgpPeer6Ipv4Unicast
- alaBgpPeer6Ipv4Multicast
- alaBgpPeer6RcvdRtRefreshMsgs
- alaBgpPeer6SentRtRefreshMsgs
- alaBgpPeer6RouteMapOut
- alaBgpPeer6RouteMapIn
- alaBgpPeer6LocalAddr
- alaBgpPeer6LastDownReason
- alaBgpPeer6LastDownTime
- alaBgpPeer6LastReadTime
- alaBgpPeer6RcvdNotifyMsgs
- alaBgpPeer6SentNotifyMsgs
- alaBgpPeer6LastSentNotifyReason
- alaBgpPeer6LastRecvNotifyReason
- alaBgpPeer6RcvdPrefixes
- alaBgpPeer6DownTransitions
alaBgpPeer6Type
alaBgpPeer6AutoReStart
alaBgpPeer6ClientStatus
alaBgpPeer6ConfedStatus
alaBgpPeer6RemovePrivateAs
alaBgpPeer6ClearCounter
alaBgpPeer6TTL
alaBgpPeer6AspathListOut
alaBgpPeer6AspathListIn
alaBgpPeer6PrefixListOut
alaBgpPeer6PrefixListIn
alaBgpPeer6CommunityListOut
alaBgpPeer6CommunityListIn
alaBgpPeer6Restart
alaBgpPeer6DefaultOriginate
alaBgpPeer6ReconfigureInBound
alaBgpPeer6ReconfigureOutBound
alaBgpPeer6MD5Key
alaBgpPeer6MD5KeyEncrypt
alaBgpPeer6RowStatus
alaBgpPeer6UpTransitions
alaBgpPeer6LastWriteTime
alaBgpPeer6AdminStatus
alaBgpPeer6State
alaBgpPeer6LocalPort
alaBgpPeer6TcpWindowSize
alaBgpPeer6ActivateIpv6
alaBgpPeer6ActivateIpv4
**show ipv6 bgp neighbors statistics**

Displays the neighbor statistics of the configured IPv6 BGP peers.

*show ipv6 bgp neighbors statistics [ipv6_address]*

---

**Syntax Definitions**

*ipv6_address*  
The 128-bit IPv6 address.

---

**Defaults**

By default, the neighbor statistics for all the IPv6 BGP peers will be displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the *ipv6_address* parameter to display the neighbor statistics of a specified IPv6 BGP peer.

---

**Examples**

```
-> show ipv6 bgp neighbors statistics
Legends:  Nbr = Neighbor
          As = Autonomous System
          RMSGS = # of received messages
          SMSGS = # of sent messages
          RUPDS = # of Update messages received
          SUPDS = # of Update messages sent
          RNOFY = # of Notify messages received
          SNOFY = # of Notify messages sent
          RPFXS = # of prefixes received
          UPTNS = # of UP transitions
          DNTNS = # of DOWN transitions

Nbr address             As    RMSGS SMSGS RUPDS SUPDS RNOFY SNOFY RPFXS UPTNS DNTNS
-----------------------+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
2001:100:3:4::1         30    225   260   2     3     0     0     10    1     1     
```

---

**output definitions**

- **Nbr address**  
The IPv6 address for this peer. This value is configured using the *ipv6 bgp neighbor* command.

- **As**  
The autonomous system to which this peer belongs. This value is configured using the *ipv6 bgp neighbor remote-as* command.
show ipv6 bgp neighbors statistics

-> show ipv6 bgp neighbors statistics 2001:100:3:4::1
Neighbor address = 2001:100:3:4::1,
# of UP transitions = 1,
Time of last UP transition = 01h:50m:36s,
# of DOWN transitions = 1,
Time of last DOWN transition = 00h:00m:00s,
Last DOWN reason = none,
# of msgs rcvd = 226,
# of Update msgs rcvd = 2,
# of prefixes rcvd = 10,
# of Route Refresh msgs rcvd = 0,
# of Notification msgs rcvd = 0,
Last rcvd Notification reason = none [none]
Time last msg was rcvd = 00h:00m:04s,
# of msgs sent = 260,
# of Update msgs sent = 3,
# of Route Refresh msgs sent = 0,
# of Notification msgs sent = 0,
Last sent Notification reason = none [none]
Time last msg was sent = 00h:00m:18s,

output definitions (continued)

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RMSGS</td>
<td>Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.</td>
</tr>
<tr>
<td>SMSGS</td>
<td>Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent by this peer.</td>
</tr>
<tr>
<td>RUPDS</td>
<td>The number of route UPDATE messages received by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.</td>
</tr>
<tr>
<td>SUPDS</td>
<td>The number of route UPDATE messages sent by this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.</td>
</tr>
<tr>
<td>RNOFY</td>
<td>The number of NOTIFY messages received by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.</td>
</tr>
<tr>
<td>SNOFY</td>
<td>The number of NOTIFY messages sent by this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.</td>
</tr>
<tr>
<td>RPFXS</td>
<td>Number of unique route prefixes received by this peer.</td>
</tr>
<tr>
<td>UPTNS</td>
<td>Number of times this peer has come up, operationally.</td>
</tr>
<tr>
<td>DNTNS</td>
<td>Number of times this peer has gone down, operationally.</td>
</tr>
</tbody>
</table>

output definitions

- **Neighbor address**: The IPv6 address for this peer. This value is configured using the `ipv6 bgp neighbor` command.
- **# of UP transitions**: Number of times this peer has come up, operationally.
- **Time of last UP transition**: The duration that this peer has been up.
- **# of DOWN transitions**: Number of times this peer has gone down, operationally.
- **Time of last DOWN transition**: The duration since this peer last went down.
**Output Definitions (continued)**

<table>
<thead>
<tr>
<th>Last DOWN reason</th>
<th>Provides a message as the last reason why a peer went down. The possible reasons for going down are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_request</td>
<td>user initiated</td>
</tr>
<tr>
<td>conn_timeout</td>
<td>connection timer expired</td>
</tr>
<tr>
<td>hold_timeout</td>
<td>hold timer expired</td>
</tr>
<tr>
<td>bad_msg</td>
<td>received a bad message from neighbor</td>
</tr>
<tr>
<td>fsm_blink</td>
<td>BGP FSM error</td>
</tr>
<tr>
<td>peer_closed</td>
<td>neighbor closed connection</td>
</tr>
<tr>
<td>peer_notify</td>
<td>neighbor sent fatal notification</td>
</tr>
<tr>
<td>tcp_error</td>
<td>Fatal TCP error</td>
</tr>
<tr>
<td>none</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th># of msgs rcvd</th>
<th>Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) received by this peer.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th># of Update msgs rcvd</th>
<th>The number of route UPDATE messages received from this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th># of prefixes rcvd</th>
<th>Number of unique route prefixes received by this peer.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th># of Route Refresh msgs rcvd</th>
<th>Number of route refresh requests this peer has received. Route refresh requests all routes learned be a peer.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th># of Notification msgs rcvd</th>
<th>Number of NOTIFY messages received from this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations.</th>
</tr>
</thead>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Last rcvd Notification reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message received from this peer. The notification reasons are listed in two parts separated by a dash (-). The following are possible notification reasons: message header error - synchronization loss message header error - bad length message header error - bad type open message error - unsupported version open message error - bad peer autonomous system open message error - bad peer bgp id open message error - unsupported option open message error - authentication failure open message error - unacceptable hold time open message error - unsupported capability update message error - malformed attribute update message error - unknown attribute update message error - missing wellknown attribute update message error - attribute flags error update message error - attribute length error update message error - invalid origin update message error - as loop update message error - invalid nexthop update message error - optional attribute error update message error - invalid network update message error - malformed aspath cease - maximum number of prefixes reached cease - administrative shutdown cease - peer de-configured cease - administrative reset cease - connection rejected cease - other configuration change cease - connection collision resolution cease - out of resources hold time out - none fsm error - none none - none</td>
<td></td>
</tr>
</tbody>
</table>

| Time last msg was rcvd | The duration since a message was received from this peer. |
| # of msgs sent | Total number of messages (UPDATE, NOTIFY, OPEN, KEEPALIVE) sent to this peer. |
| # of Update msgs sent | Number of route UPDATE messages sent to this peer. UPDATE messages contain route reachability information, BGP attributes, and route feasibility information. |
| # of Route Refresh msgs sent | Number of route refresh requests this peer has sent. Route refresh requests request all routes learned be a peer. |
| # of Notification msgs sent | Number of NOTIFY messages sent to this peer. NOTIFY messages contain error information, such as unsupported parameters, invalid attributes, and holdtime expirations. |
output definitions (continued)

| Last sent Notification reason | NOTIFY messages include errors codes. These error codes are listed in this field. They apply to the last NOTIFY message sent by this peer. The notification reasons are listed in two parts separated by a dash (-). See the list of possible notification reasons under the description for the Peer last received notification reason field above. |
| Time last msg was sent         | The duration since a message was sent to this peer. |

Release History

Release 7.1.1; command was introduced.

Related Commands

`show ipv6 bgp neighbors` Displays the configured IPv6 BGP peers.

MIB Objects

- `alaBgpPeer6Table`
  - `alaBgpPeer6Addr`
  - `alaBgpPeer6RcvdMsgs`
  - `alaBgpPeer6SentMsgs`
  - `alaBgpPeer6RcvdUpdMsgs`
  - `alaBgpPeer6SentUpdMsgs`
  - `alaBgpPeer6LastTransitionTime`
  - `alaBgpPeer6LastUpTime`
  - `alaBgpPeer6BgpId`
  - `alaBgpPeer6LocalIntfName`
  - `alaBgpPeer6RestartTime`
  - `alaBgpPeer6RestartState`
  - `alaBgpPeer6RestartFwdState`
  - `alaBgpPeer6Ipv6Unicast`
  - `alaBgpPeer6HoldTime`
  - `alaBgpPeer6KeepAlive`
  - `alaBgpPeer6ConnRetryInterval`
  - `alaBgpPeer6HoldTimeConfigured`
  - `alaBgpPeer6KeepAliveConfigured`
  - `alaBgpPeer6Ipv4NextHop`
  - `alaBgpPeer6Ipv6NextHop`
**show ipv6 bgp neighbors policy**

Displays the incoming and outgoing prefix6 list policy identifiers configured for BGP IPv6 peer.

**show ipv6 bgp neighbors policy ipv6_address**

---

**Syntax Definitions**

*ipv6_address* The 128-bit IPv6 address.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

This command displays all of the configured policies for the router, or the policies configured for a specific BGP IPv6 peer.

---

**Examples**

```
-> show ipv6 bgp neighbors policy
Neighbor address = 2001::1,
    Neighbor autonomous system = 1,
    Neighbor output policy map name = <none>,
    Neighbor input policy map name = <none>,
    Neighbor output aspath-list name = <none>,
    Neighbor input aspath-list name = <none>,
    Neighbor output prefix-list name = <none>,
    Neighbor input prefix-list name = <none>,
    Neighbor output community-list name = <none>,
    Neighbor input community-list name = <none>,
    Neighbor soft reconfiguration = enabled
    Neighbor output prefix6-list name = <none>,
    Neighbor input prefix6-list name = <none>
```

---

**output definitions**

- **Neighbor autonomous system** The AS to which the peer is assigned. This can be assigned by using the `ipv6 bgp neighbor remote-as` command.

- **Neighbor output policy map name** The outbound route map policy for the peer. This can be assigned by using the `ipv6 bgp neighbor route-map` command.
**Neighbor input policy map name**
The inbound route map policy for the peer. This can be assigned by using the `ipv6 bgp neighbor route-map` command.

**Neighbor output aspath-list name**
The outbound AS path list policy for the peer. This can be assigned by using the `ipv6 bgp neighbor out-aspathlist` command.

**Neighbor input aspath-list name**
The inbound AS path list policy for the peer. This can be assigned by using the `ipv6 bgp neighbor in-aspathlist` command.

**Neighbor output prefix-list name**
The outbound prefix list policy for the peer. This can be assigned by using the `ipv6 bgp neighbor out-prefixlist` command.

**Neighbor input prefix-list name**
The inbound prefix list policy for the peer. This can be assigned by using the `ipv6 bgp neighbor in-prefixlist` command.

**Neighbor output community-list name**
The outbound community list policy for the peer. This can be assigned by using the `ipv6 bgp neighbor out-communitylist` command.

**Neighbor input community-list name**
The inbound community list policy for the peer. This can be assigned by using the `ipv6 bgp neighbor in-communitylist` command.

**Neighbor soft reconfiguration**
Lists whether soft reconfigurations are enabled or disabled for this peer. This is configured using the `ipv6 bgp neighbor soft-reconfiguration` command.

**Neighbor output prefix6-list name**
The outbound prefix6-list policy for the peer. This is configured using the `ipv6 bgp neighbor out-prefix6list` command.

**Neighbor input prefix6-list name**
The inbound prefix6-list policy for the peer. This is configured using the `ipv6 bgp neighbor in-prefix6list` command.

**Release History**
Release 7.1.1; command was introduced.

**Related Commands**

- `show ipv6 bgp neighbors` Displays configured IPv6 BGP peers

**MIB Objects**

- `alaBgpPeer6Table`
- `alaBgpPeer6AS`
- `alaBgpPeer6RouteMapOut`
- `alaBgpPeer6RouteMapIn`
- `alaBgpPeer6AspathListOut`
- `alaBgpPeer6AspathListIn`
- `alaBgpPeer6PrefixListOut`
- `alaBgpPeer6PrefixListIn`
- `alaBgpPeer6CommunityListOut`
- `alaBgpPeer6CommunityListIn`
- `alaBgpPeer6SoftReconfig`
- `alaBgpPeer6Prefix6ListOut`
- `alaBgpPeer6Prefix6ListIn`
**show ipv6 bgp neighbors timers**

Displays the timers for configured IPv6 BGP peers.

*Syntax*

```plaintext
show ipv6 bgp neighbors timers [ipv6_address]
```

**Syntax Definitions**

- `ipv6_address`: The 128-bit IPv6 address.

**Defaults**

By default, the timer values for all the IPv6 BGP peers will be displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6_address` parameter to display the timer value for a specified IPv6 BGP peer.

**Examples**

```
--> show ipv6 bgp neighbors timers
```

**output definitions**

- **Nbr address**: The IPv6 address for this BGP peer. Assign this address using the `ipv6 bgp neighbor` command.
- **As**: The autonomous system to which this peer belongs. A peer’s AS number is assigned using the `ipv6 bgp neighbor remote-as` command.
- **Hold**: The actual negotiated hold time value.
- **Hold (C)**: The hold time value. This value is configured using the `ipv6 bgp neighbor timers` command.
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`show ip bgp statistics` Displays BGP global statistics.

**MIB Objects**

- `alaBgpPeer6Table`
- `alaBgpPeer6Addr`
- `alaBgpPeer6ConnRetryInterval`
- `alaBgpPeer6MinRouteAdvertisementInterval`
- `alaBgpPeer6HoldTime`

---

**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RtAdv</td>
<td>The route advertisement interval, in seconds, for updates between external BGP peers.</td>
</tr>
<tr>
<td>Retry</td>
<td>The interval, in seconds, between retries by this peer to set up a connection through TCP with another peer. This value is configured using the <code>ipv6 bgp neighbor timers</code> command.</td>
</tr>
<tr>
<td>Kalive</td>
<td>The actual negotiated value, in seconds, between KEEPALIVE messages. KEEPALIVE messages do not contain route or status updates; they serve only to tell other peers that the connection is still live and this peer is reachable.</td>
</tr>
<tr>
<td>Ka (C)</td>
<td>The KEEPALIVE interval as configured using the <code>ipv6 bgp neighbor timers</code> command.</td>
</tr>
</tbody>
</table>
Server Load Balancing (SLB) allows clients to send requests to servers logically grouped together in clusters. Each cluster logically aggregates a set of servers running identical applications with access to the same content (for example, web servers). Clients access clusters through the use of a Virtual IP (VIP) address.

MIB information for the SLB commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>ALCATEL-IND1-SLB-MIB.mib</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>alcatelIND1SLBMIB</td>
</tr>
</tbody>
</table>

A summary of available commands is listed here:

| Global SLB Commands                      | ip slb admin-state       |
|                                         | ip slb reset statistics  |
|                                         | show ip slb              |

| SLB Cluster Commands                     | ip slb cluster           |
|                                         | ip slb cluster admin-state|
|                                         | ip slb cluster ping period|
|                                         | ip slb cluster ping timeout|
|                                         | ip slb cluster ping retries|
|                                         | ip slb cluster probe     |
|                                         | show ip slb clusters     |
|                                         | show ip slb cluster      |

| SLB Server Commands                      | ip slb server ip cluster |
|                                         | ip slb server ip cluster probe |
|                                         | show ip slb cluster server  |
|                                         | show ip slb servers        |

| SLB Probe Commands                       | ip slb probe             |
|                                         | ip slb probe timeout     |
|                                         | ip slb probe period      |
|                                         | ip slb probe port        |
|                                         | ip slb probe retries     |
|                                         | ip slb probe username    |
|                                         | ip slb probe password    |
|                                         | ip slb probe url         |
|                                         | ip slb probe status      |
|                                         | ip slb probe send        |
|                                         | ip slb probe expect      |
|                                         | show ip slb probes       |
ip slb admin-state

Enables or disables the administrative status for Server Load Balancing (SLB) on a switch.

ip slb admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the administrative status for Server Load Balancing.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the administrative status for Server Load Balancing on the switch.</td>
</tr>
</tbody>
</table>

Defaults

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Disabling the administrative status for the SLB feature does not delete the SLB configuration from the switch. The next time the feature is enabled, the existing configuration becomes active.

Examples

-> ip slb admin-state enable
-> ip slb admin-state disable

Release History

Release 7.1.1; command introduced.
Related Commands

- **show ip slb**: Displays the status of Server Load Balancing on a switch.
- **ip slb cluster**: Configures a Server Load Balancing cluster on a switch.
- **ip slb server ip cluster**: Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

- **slbFeatureGroup**
- **slbAdminStatus**
**ip slb reset statistics**

Resets SLB statistics for all clusters configured on the switch.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Note that the *qos apply* command resets both QoS statistics and SLB cluster statistics. The *ip slb reset statistics* command only resets SLB statistics.

**Examples**

`-> ip slb reset statistics`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show ip slb clusters`: Displays the status and configuration of all Server Load Balancing clusters on a switch.
- `show ip slb cluster`: Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

**MIB Objects**

- `slbFeatureGroup`: Provides information about the SLB feature.
- `slbResetStatistics`: Contains information about the reset of SLB statistics.
ip slb cluster

Configures a Server Load Balancing (SLB) cluster on a switch.

**ip slb cluster** name {vip ip_address | condition string} [l3 | l2]

**no ip slb cluster** name

---

**Syntax Definitions**

- **name**
  The name of the Server Load Balancing (SLB) cluster. The name can consist a maximum of 23 characters. Names with spaces must be enclosed within quotation marks (for example, “mail server”).

- **ip_address**
  The Virtual IP (VIP) address for the Server Load Balancing cluster. This IP address must be in dotted decimal format.

- **string**
  The name of an existing QoS policy condition that identifies the Server Load Balancing cluster.

- **l3**
  Specifies Layer 3 Server Load Balancing mode. The source and destination MAC and TTL of each packet is modified before the packet is bridged or routed to the server.

- **l2**
  Specifies Layer 2 Server Load Balancing mode. Packets are not modified before they are bridged to the server. This parameter is only available when using the **condition** parameter.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>l3</td>
<td>l3</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to delete a Server Load Balancing cluster.

- Once a cluster is created, the Virtual IP or condition cannot be modified. To modify these values, delete the cluster and re-create the cluster with the different VIP and conditions.

- The VIP address of the SLB cluster **must** be an address that is in the same subnet as the servers.
Specifying the l3 parameter when configuring a VIP cluster is not required. VIP clusters only use the Layer-3 mode to route traffic to the servers. Layer-2 mode is not supported with this type of cluster.

The QoS policy condition must exist before it is assigned to an SLB cluster. Use the policy condition command to create the QoS policy condition. See the “QoS Policy Commands” chapter for more information.

SLB clusters are not active if the Server Load Balancing feature is disabled for the switch. Use the ip slb admin-state command to enable this feature.

Note. It is possible to configure clusters and add or remove servers from a cluster even when SLB is disabled for the switch.

Examples

-> ip slb cluster corporate_servers vip 1.2.3.4
-> ip slb cluster "mail servers" vip 1.2.3.6
-> ip slb cluster cluster_1 condition intranet_cond l2
-> ip slb cluster cluster_2 condition slb_cond l3
-> no ip slb cluster hr_servers

Release History

Release 7.1.1; command introduced.

Related Commands

show ip slb clusters
Displays the status and configuration of all Server Load Balancing clusters on a switch.

show ip slb cluster
Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

ip slb admin-state
Enables or disables Server Load Balancing on a switch.

ip slb server ip cluster
Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

slbClusterTable
  slbClusterName
  slbClusterVIP
  slbClusterRowStatus
  slbClusterPackets
  slbClusterCondition
  slbClusterType
ip slb cluster admin-state

Administratively enables or disables a Server Load Balancing (SLB) cluster on a switch.

`ip slb cluster cluster_name admin-state {enable | disable}

Syntax Definitions

- `cluster_name` The name of an existing Server Load Balancing cluster.
- `enable` Administratively enables a Server Load Balancing cluster on a switch.
- `disable` Administratively disables a Server Load Balancing cluster on a switch.

Defaults

By default, a cluster is administratively enabled when the cluster is created.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

The SLB cluster name specified with this command must already exist in the switch configuration.

Examples

- `-> ip slb cluster hr_servers admin-state enable`
- `-> ip slb cluster "mail servers" admin-state disable`

Release History

Release 7.1.1; command introduced.
Related Commands

- **show ip slb clusters**: Displays the status and configuration of all Server Load Balancing clusters on a switch.
- **show ip slb cluster**: Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
- **ip slb cluster**: Configures Server Load Balancing clusters.
- **ip slb server ip cluster**: Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

MIB Objects

- slbClusterTable
  - slbClusterAdminStatus
**ip slb cluster ping period**

Modifies the number of seconds to check the health of the servers in a Server Load Balancing (SLB) cluster.

```
ip slb cluster cluster_name ping period seconds
```

### Syntax Definitions

- **cluster_name**: The name of the Server Load Balancing cluster.
- **seconds**: The number of seconds for the ping period. Specifying 0 (zero) disables the ping.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/X48C4E/V48C8/C32/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you do not set the ping period to zero, then the ping period must be greater than or equal to the ping timeout value divided by 1000. Use the **ip slb cluster ping timeout** command to modify the ping timeout value.

### Examples

```
-> ip slb cluster hr_servers ping period 120
-> ip slb cluster "mail servers" ping period 0
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- **show ip slb clusters**
  Displays the status and configuration of all Server Load Balancing clusters on a switch.

- **show ip slb cluster**
  Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

- **ip slb cluster ping timeout**
  Modifies the ping timeout value.

- **ip slb cluster ping retries**
  Modifies the number of ping retries.

**MIB Objects**

- **slbClusterTable**
  slbClusterPingPeriod
ip slb cluster ping timeout

Configures the ping timeout value for a Server Load Balancing (SLB) cluster before it retries.

```
ip slb cluster cluster_name ping timeout milliseconds
```

**Syntax Definitions**

- `cluster_name` The name of the Server Load Balancing cluster.
- `milliseconds` The number of milliseconds for the ping timeout. The valid range for the ping timeout value is 0 to 1000 times the ping period. For example, if the ping period is 10 seconds, then maximum value for the ping timeout is 10000.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliseconds</td>
<td>3000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip slb cluster ping period` command to modify the ping period value.

**Examples**

- `-> ip slb cluster "mail servers" ping timeout 1000`
- `-> ip slb cluster hr_servers ping timeout 6000`

**Release History**

Release 7.1.1; command introduced.
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip slb clusters</code></td>
<td>Displays the status and configuration of all Server Load Balancing clusters on a switch.</td>
</tr>
<tr>
<td><code>show ip slb cluster</code></td>
<td>Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.</td>
</tr>
<tr>
<td><code>ip slb cluster ping period</code></td>
<td>Modifies the ping period value.</td>
</tr>
<tr>
<td><code>ip slb cluster ping retries</code></td>
<td>Modifies the number of ping retries.</td>
</tr>
</tbody>
</table>

MIB Objects

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slbClusterTable</td>
<td></td>
</tr>
<tr>
<td>slbClusterPingTimeout</td>
<td></td>
</tr>
</tbody>
</table>
ip slb cluster ping retries

Configures the number of ping attempts for a Server Load Balancing (SLB) cluster.

ip slb cluster *cluster_name* ping retries *count*

**Syntax Definitions**

- *cluster_name*: The name of the Server Load Balancing cluster.
- *count*: The number of ping retries.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>count</em></td>
<td>3</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- -> ip slb cluster "mail servers" ping retries 5
- -> ip slb cluster hr_servers ping retries 10

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **show ip slb clusters**
  Displays the status and configuration of all Server Load Balancing clusters on a switch.

- **show ip slb cluster**
  Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

- **ip slb cluster ping period**
  Modifies the ping period value.

- **ip slb cluster ping timeout**
  Modifies the ping timeout value.

MIB Objects

- **slbClusterTable**
  - **slbClusterPingRetries**
**ip slb cluster probe**

Configures a probe for a Server Load Balancing (SLB) cluster.

```
ip slb cluster cluster_name probe probe_name
```

**Syntax Definitions**

- `cluster_name`  The name of the Server Load Balancing cluster.
- `probe_name`    The name of the Server Load Balancing (SLB) probe.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must create the probe with the `ip slb probe` before you can use this command.

**Examples**

```
-> ip slb cluster mail_servers probe mail_server_probe
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show ip slb clusters` Displays the status and configuration of all Server Load Balancing clusters on a switch.
- `ip slb probe` Configures and deletes SLB probes.
- `show ip slb cluster` Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
- `ip slb server ip cluster` Adds, deletes, or modifies parameters of physical servers in logical Server Load Balancing clusters.

**MIB Objects**

- `slbClusterTable`
slbClusterProbeName
**ip slb server ip cluster**

Adds a physical server to a Server Load Balancing (SLB) cluster, deletes a physical server from an SLB cluster, or modifies the administrative status of a physical server in an SLB cluster.

```
ip slb server ip ip_address cluster cluster_name [admin-state {enable | disable}] [weight weight]
no ip slb server ip ip_address cluster cluster_name
```

**Syntax Definitions**

- `ip_address` The IP address for the physical server.
- `cluster_name` The name of an existing Server Load Balancing cluster.
- `enable` Enables a server.
- `disable` Disables a server.
- `weight` Specifies the weight of the server.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>weight</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a physical server from a Server Load Balancing cluster.

- Use the weight parameter to assign the server preference value. Each server or server cluster can be assigned a weight to set their preference value for distribution of incoming network traffic. The weights assigned are relative. For example, if Servers A and B have respective weights of 10 and 20 within a cluster, Server A would get half the traffic of Server B.

- Assigning a weight of 0 (zero) to a server prevents the server from being assigned any new connections. This server is a backup server.

- A higher weight value indicates that the server can accept more network traffic.
**Examples**

-> ip slb server ip 10.255.11.127 cluster corporate_servers
-> ip slb server ip 10.255.11.109 cluster "mail servers" admin-state enable weight 5
-> no ip slb server ip 10.255.11.105 cluster hr_servers

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show ip slb clusters` Displays the status and configuration of all Server Load Balancing clusters on a switch.
- `show ip slb cluster` Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
- `ip slb admin-state` Enables or disables Server Load Balancing on a switch.
- `ip slb cluster` Configures Server Load Balancing clusters.

**MIB Objects**

- `slbServerTable`
  - `slbServerRowStatus`
  - `slbServerAdminStatus`
  - `slbServerAdminWeight`
ip slb server ip cluster probe

Configures a probe for a Server Load Balancing (SLB) server.

`ip slb server ip ip_address cluster cluster_name probe probe_name`

**Syntax Definitions**

- `ip_address`: The IP address for the physical server.
- `cluster_name`: The name of the Server Load Balancing cluster.
- `probe_name`: The name of the Server Load Balancing probe.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must create the probe with the `ip slb probe` before you can use this command.

**Examples**

- `-> ip slb server ip 10.255.11.127 cluster corporate_servers probe p_http`

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- `show ip slb clusters`  Displays the status and configuration of all Server Load Balancing clusters on a switch.
- `show ip slb cluster`  Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.
- `ip slb probe`  Configures and deletes SLB probes.
- `ip slb admin-state`  Enables or disables Server Load Balancing on a switch.
- `ip slb cluster`  Configures Server Load Balancing clusters.

**MIB Objects**

- `slbServerTable`
  - `slbServerProbeName`
ip slb probe

Configures a Server Load Balancing (SLB) probe used to check the health of servers or clusters.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
```

```
no ip slb probe probe_name
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th><strong>probe_name</strong></th>
<th>Specifies the name of the Server Load Balancing probe.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ftp</strong></td>
<td>Specifies an FTP probe.</td>
</tr>
<tr>
<td><strong>http</strong></td>
<td>Specifies an HTTP probe.</td>
</tr>
<tr>
<td><strong>https</strong></td>
<td>Specifies an HTTPS probe.</td>
</tr>
<tr>
<td><strong>imap</strong></td>
<td>Specifies an IMAP probe.</td>
</tr>
<tr>
<td><strong>imaps</strong></td>
<td>Specifies an IMAPS probe.</td>
</tr>
<tr>
<td><strong>nntp</strong></td>
<td>Specifies an NNTP probe.</td>
</tr>
<tr>
<td><strong>ping</strong></td>
<td>Specifies a ping probe.</td>
</tr>
<tr>
<td><strong>pop</strong></td>
<td>Specifies a POP probe.</td>
</tr>
<tr>
<td><strong>pops</strong></td>
<td>Specifies a POPS probe.</td>
</tr>
<tr>
<td><strong>smtp</strong></td>
<td>Specifies an SMTP probe.</td>
</tr>
<tr>
<td><strong>tcp</strong></td>
<td>Specifies a TCP probe.</td>
</tr>
<tr>
<td><strong>udp</strong></td>
<td>Specifies a UDP probe.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to delete an SLB probe.

**Examples**

```
-> ip slb probe mail_server_probe smtp
-> no ip slb probe mail_server_probe
```
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`show ip slb probes` Displays the configuration of SLB probes.

**MIB Objects**

`slbProbeTable`
- `slbProbeName`
- `slbProbeMethod`
ip slb probe timeout

Configures the amount of time to wait for Server Load Balancing (SLB) probe answers.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} timeout seconds
```

**Syntax Definitions**

- `probe_name` 
  Specifies the name of the Server Load Balancing probe.
- `ftp` 
  Specifies an FTP probe.
- `http` 
  Specifies an HTTP probe.
- `https` 
  Specifies an HTTPS probe.
- `imap` 
  Specifies an IMAP probe.
- `imaps` 
  Specifies an IMAPS probe.
- `nntp` 
  Specifies an NNTP probe.
- `ping` 
  Specifies a ping probe.
- `pop` 
  Specifies a POP probe.
- `pops` 
  Specifies a POPS probe.
- `smtp` 
  Specifies an SMTP probe.
- `tcp` 
  Specifies a TCP probe.
- `udp` 
  Specifies a UDP probe.
- `seconds` 
  Specifies the timeout in seconds.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>3000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C4E/V48C8/C32E/T24C2/X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A
**Examples**

-> ip slb probe mail_server smtp timeout 12000

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `ip slb probe` Configures and deletes SLB probes.
- `show ip slb probes` Displays the configuration of SLB probes.

**MIB Objects**

- `slbProbeTable`
  - `slbProbeName`
  - `slbProbeMethod`
  - `slbProbeTimeout`
**ip slb probe period**

Configures the length of time between each SLB probe to check the health of the servers.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} period seconds
```

**Syntax Definitions**

- `probe_name`: Specifies the name of the Server Load Balancing probe.
- `ftp`: Specifies an FTP probe.
- `http`: Specifies an HTTP probe.
- `https`: Specifies an HTTPS probe.
- `imap`: Specifies an IMAP probe.
- `imaps`: Specifies an IMAPS probe.
- `nntp`: Specifies an NNTP probe.
- `ping`: Specifies a ping probe.
- `pop`: Specifies a POP probe.
- `pops`: Specifies a POPS probe.
- `smtp`: Specifies an SMTP probe.
- `tcp`: Specifies a TCP probe.
- `udp`: Specifies a UDP probe.
- `seconds`: Specifies the length of time for the SLB probe period.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A
Examples

-> ip slb probe web_server http period 120

Release History

Release 7.1.1; command introduced.

Related Commands

- ip slb probe
  Configures and deletes SLB probes.
- show ip slb probes
  Displays the configuration of SLB probes.

MIB Objects

- slbProbeTable
  slbProbeName
  slbProbeMethod
  slbProbePeriod
**ip slb probe port**

Configures the TCP/UDP port on which the Server Load Balancing (SLB) probe is sent.

```plaintext
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} port port_number
```

### Syntax Definitions

- **probe_name**: Specifies the name of the Server Load Balancing probe.
- **ftp**: Specifies an FTP probe.
- **http**: Specifies an HTTP probe.
- **https**: Specifies an HTTPS probe.
- **imap**: Specifies an IMAP probe.
- **imaps**: Specifies an IMAPS probe.
- **nntp**: Specifies an NNTP probe.
- **ping**: Specifies a ping probe.
- **pop**: Specifies a POP probe.
- **pops**: Specifies a POPS probe.
- **smtp**: Specifies an SMTP probe.
- **tcp**: Specifies a TCP probe.
- **udp**: Specifies a UDP probe.
- **port_number**: Specifies the TCP/UDP port number.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>port_number</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A
**Examples**

```
-> ip slb probe mis_server udp port 200
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip slb probe</td>
<td>Configures and deletes SLB probes.</td>
</tr>
<tr>
<td>show ip slb probes</td>
<td>Displays the configuration of SLB probes.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- slbProbeTable
  - slbProbeName
  - slbProbeMethod
  - slbProbePort
ip slb probe retries

Configures the number of Server Load Balancing (SLB) probe retries that are performed before deciding that a server is out of service.

```
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} retries retries
```

Syntax Definitions

- `probe_name`: Specifies the name of the Server Load Balancing probe.
- `ftp`: Specifies an FTP probe.
- `http`: Specifies an HTTP probe.
- `https`: Specifies an HTTPS probe.
- `imap`: Specifies an IMAP probe.
- `imaps`: Specifies an IMAPS probe.
- `nntp`: Specifies an NNTP probe.
- `ping`: Specifies a ping probe.
- `pop`: Specifies a POP probe.
- `pops`: Specifies a POPS probe.
- `smtp`: Specifies an SMTP probe.
- `tcp`: Specifies a TCP probe.
- `udp`: Specifies a UDP probe.
- `retries`: Specifies the number of retries.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>retries</td>
<td>3</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A
Examples

-> ip slb probe mail_server smtp retries 5

Release History

Release 7.1.1; command introduced.

Related Commands

- ip slb probe: Configures and deletes SLB probes.
- show ip slb probes: Displays the configuration of SLB probes.

MIB Objects

- slbProbeTable
- slbProbeName
- slbProbeMethod
- slbProbeRetries
**ip slb probe username**

Configures a user name that is sent to a server as credentials for an HTTP GET operation to verify the health of the server.

```plaintext
ip slb probe probe_name {http | https} username user_name
```

**Syntax Definitions**

- `probe_name` Specifies the name of the Server Load Balancing probe.
- `http` Specifies an HTTP probe.
- `https` Specifies an HTTPS probe.
- `user_name` Specifies user name.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T48C2</th>
<th>X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```plaintext
-> ip slb probe web_server http username subnet1
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `ip slb probe` Configures and deletes SLB probes.
- `show ip slb probes` Displays the configuration of SLB probes.

**MIB Objects**

- `slbProbeTable`
  - `slbProbeName`
  - `slbProbeMethod`
slbProbeHttpUsername
**ip slb probe password**

Configures a password that is sent to a server as credentials for an HTTP GET to verify the health of the server.

```
ip slb probe probe_name {http | https} password password
```

**Syntax Definitions**

- `probe_name`: Specifies the name of the Server Load Balancing probe.
- `http`: Specifies an HTTP probe.
- `https`: Specifies an HTTPS probe.
- `password`: Specifies the password.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The password is encrypted in the configuration file so that it is not readable.

**Examples**

```
-> ip slb probe web_server http password hlf45xc
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `ip slb probe`: Configures and deletes SLB probes.
- `show ip slb probes`: Displays the configuration of SLB probes.

**MIB Objects**

- `slbProbeTable`
  - `slbProbeName`
  - `slbProbeMethod`
slbProbeHttpPassword
**ip slb probe url**

Configures a URL that is sent to a server for an HTTP GET to verify the health of the server.

```
ip slb probe probe_name {http | https} url url
```

### Syntax Definitions

- **probe_name**: Specifies the name of the Server Load Balancing probe.
- **http**: Specifies an HTTP probe.
- **https**: Specifies an HTTPS probe.
- **url**: Specifies the URL of the server.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> ip slb probe web_server http url pub/index.html
```

### Release History

Release 7.1.1; command introduced.

### Related Commands

- **ip slb probe**: Configures and deletes SLB probes.
- **show ip slb probes**: Displays the configuration of SLB probes.

### MIB Objects

- `slbProbeTable`
- `slbProbeName`
- `slbProbeMethod`
slbProbeHttpUrl
ip slb probe status

Configures the expected status returned from an HTTP GET to verify the health of a server.

ip slb probe probe_name {http | https} status status_value

---

**Syntax Definitions**

- **probe_name**: Specifies the name of the Server Load Balancing probe.
- **http**: Specifies an HTTP probe.
- **https**: Specifies an HTTPS probe.
- **status_value**: Specifies the expected status returned.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_value</td>
<td>200</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

---

**Usage Guidelines**

N/A

---

**Examples**

```
-> ip slb probe web_server http status 404
```

---

**Release History**

Release 7.1.1; command introduced.
### Related Commands

- **ip slb probe**
  - Configures and deletes SLB probes.
- **show ip slb probes**
  - Displays the configuration of SLB probes.

### MIB Objects

- **slbProbeTable**
  - slbProbeName
  - slbProbeMethod
  - slbProbePeriod
  - slbProbeHttpStatus
**ip slb probe send**

Configures an ASCII string that is sent to a server to invoke a server response and verify the health of the server.

```
ip slb probe probe_name {tcp | udp} send send_string
```

**Syntax Definitions**

- **probe_name**: Specifies the name of the Server Load Balancing probe.
- **tcp**: Specifies a TCP probe.
- **udp**: Specifies a UDP probe.
- **send_string**: Specifies the ASCII string sent to a server to invoke a response.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

NA

**Examples**

```
-> ip slb probe web_server tcp send test
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **ip slb probe**: Configures and deletes SLB probes.
- **show ip slb probes**: Displays the configuration of SLB probes.

**MIB Objects**

- **slbProbeTable**
  - **slbProbeName**
  - **slbProbeMethod**
slbProbeSend
**ip slb probe expect**

Configures an ASCII string used to compare a response from a server to verify the health of the server.

```
ip slb probe probe_name {http | https | tcp | udp} expect expect_string
```

### Syntax Definitions

- `probe_name` Specifies the name of the Server Load Balancing probe.
- `http` Specifies an HTTP probe.
- `https` Specifies an HTTPS probe.
- `tcp` Specifies a TCP probe.
- `udp` Specifies a UDP probe.
- `expect_string` Specifies the ASCII string used to compare a response from a server.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> ip slb probe web_server http expect test
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- `ip slb probe` Configures and deletes SLB probes.
- `show ip slb probes` Displays the configuration of SLB probes.

**MIB Objects**

- `slbProbeTable`
  - `slbProbeName`
  - `slbProbeMethod`
  - `slbProbeExpect`
show ip slb

Displays the status of Server Load Balancing on a switch.

show ip slb

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ip slb

Admin status : Enabled,
Operational status : In Service,
Number of clusters = 3

output definitions

Admin status The current administrative status of Server Load Balancing (SLB) on this switch (Enabled or Disabled).
Operational status The current operational status of Server Load Balancing (SLB) on this switch, which is either In service (at least one SLB cluster is in service) or Out of service (all SLB clusters are out of service).
Number of clusters The total number of Server Load Balancing (SLB) clusters on this switch.

Release History

Release 7.1.1; command introduced.
Related Commands

**show ip slb servers**  
Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.

**show ip slb clusters**  
Displays the status and configuration of all Server Load Balancing clusters on a switch.

**show ip slb cluster**  
Displays detailed status and configuration information for a single Server Load Balancing cluster on a switch.

**show ip slb cluster server**  
Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.

MIB Objects

**slbFeature**

- **slbAdminStatus**
- **slbOperStatus**
- **slbClustersCount**
show ip slb clusters

Displays the status and basic configuration for all Server Load Balancing (SLB) clusters on a switch. This command also displays traffic statistics for QoS policy condition clusters.

show ip slb clusters [statistics]

Syntax Definitions

statistics Displays SLB statistics for QoS policy condition clusters.

Defaults

By default, the status and basic configuration for all clusters is displayed; statistics are not shown.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the statistics parameter to display the total number of packets that were passed to clusters because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below.

Examples

-> show ip slb clusters

<table>
<thead>
<tr>
<th>Cluster Name</th>
<th>VIP/COND</th>
<th>Admin Status</th>
<th>Operational Status</th>
<th># Srv</th>
<th>% Avail</th>
</tr>
</thead>
<tbody>
<tr>
<td>WorldWideWeb</td>
<td>128.241.130.204</td>
<td>Enabled</td>
<td>In Service</td>
<td>3</td>
<td>95</td>
</tr>
<tr>
<td>Intranet</td>
<td>128.241.130.205</td>
<td>Enabled</td>
<td>In Service</td>
<td>2</td>
<td>100</td>
</tr>
<tr>
<td>FileTransfer</td>
<td>128.241.130.206</td>
<td>Enabled</td>
<td>Out of Service</td>
<td>2</td>
<td>50</td>
</tr>
</tbody>
</table>

output definitions

Cluster Name The name of the SLB cluster.

VIP/COND The virtual IP (VIP) address or the policy condition name for the SLB cluster.

Admin Status The administrative status of the SLB cluster (Enabled or Disabled).

Operational Status The operational status of the SLB cluster; In Service (at least one physical server is operational in the cluster) or Out of Service.
Server Load Balancing Commands

```
-> show ip slb clusters statistics

<table>
<thead>
<tr>
<th>Cluster Name</th>
<th>Admin Status</th>
<th>Operational Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster1</td>
<td>Enabled</td>
<td>In Service</td>
<td>4 Servers</td>
</tr>
<tr>
<td>Cluster2</td>
<td>Enabled</td>
<td>In Service</td>
<td>4 Servers</td>
</tr>
</tbody>
</table>

Dst IP 101.113.113.1/255.255.255.255              4503911
Src IP 202.202.1.0/255.255.255.0                 6527831
Src Port 2/49
```

**output definitions**

<table>
<thead>
<tr>
<th># Srv</th>
<th>The total number of physical servers that belong to the SLB cluster.</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Avail</td>
<td>The percentage of time that the physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.</td>
</tr>
</tbody>
</table>

**output definitions (continued)**

Cluster Name

The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.

Admin Status

The administrative state of this physical server (Enabled or Disabled).

Operational Status

The operational state of this server. The possible states are described as follows:

- **Disabled** (this server is administratively disabled).
- **No Answer** (this server has not responded to ping requests).
- **Link Down** (there is a bad connection to this server).
- **In Service** (this server is used for SLB cluster client connections).
- **Discovery** (the SLB cluster is pinging this physical server).
- **Retrying** (the SLB cluster is making another attempt to bring up this server).

Count

The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.

Dst

The destination Virtual IP address assigned to the cluster.

Src

Source IP address assigned to the cluster.

Src Port

Source slot and port number of the SLB cluster.

**Release History**

Release 7.1.1; command introduced.
Related Commands

- `ip slb reset statistics`  Resets SLB statistics for all clusters.
- `show ip slb cluster`  Displays detailed status and configuration information for a single SLB cluster.
- `show ip slb servers`  Displays the status of all physical servers belonging to each SLB cluster on a switch.
- `show ip slb cluster server`  Displays detailed status and configuration information for a single physical server in an SLB cluster.

MIB Objects

- `slbClusterTable`
  - `slbClusterName`
  - `slbClusterVIP`
  - `slbClusterCondition`
  - `slbClusterAdminStatus`
  - `slbClusterOperStatus`
  - `slbClusterNumberOfServers`
  - `slbClusterNewFlows`
- `slbStatsTable`
  - `slbStatsClusterName`
  - `slbStatsIndex`
  - `slbStatsCounter`
- `slbStatsQualTable`
  - `slbStatsQualType`
  - `slbStatsQualData`
**show ip slb cluster**

Displays detailed statistics and configuration information and operational status for a single Server Load Balancing (SLB) cluster. This command also displays traffic statistics for single QoS policy condition cluster.

**show ip slb cluster name [statistics]**

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the SLB cluster.</td>
</tr>
<tr>
<td>statistics</td>
<td>Displays SLB statistics for the specified cluster.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `statistics` parameter to display the total number of packets that were passed to the cluster because they met the QoS condition criteria configured for that cluster. The polling interval used to obtain such statistics is every 15 minutes. See the second example below:

### Examples

```bash
-> show ip slb cluster Intranet
```

Cluster Intranet

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP</td>
<td>128.241.130.204,</td>
</tr>
<tr>
<td>Type</td>
<td>L3</td>
</tr>
<tr>
<td>Admin status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Operational status</td>
<td>In Service</td>
</tr>
<tr>
<td>Ping period (seconds)</td>
<td>60,</td>
</tr>
<tr>
<td>Ping timeout (milliseconds)</td>
<td>3000,</td>
</tr>
<tr>
<td>Ping retries</td>
<td>3,</td>
</tr>
<tr>
<td>Probe</td>
<td>None,</td>
</tr>
<tr>
<td>Number of packets</td>
<td>25346,</td>
</tr>
<tr>
<td>Number of servers</td>
<td>3,</td>
</tr>
</tbody>
</table>

Server 128.241.130.107

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin status</td>
<td>Enabled</td>
</tr>
<tr>
<td>Operational status</td>
<td>In Service</td>
</tr>
<tr>
<td>Weight</td>
<td>4,</td>
</tr>
<tr>
<td>Availability (%)</td>
<td>0</td>
</tr>
</tbody>
</table>

Server 128.241.130.117
Admin status = Enabled, Operational status = Discovery,
Weight = 6, Availability (%) = 0
Server 128.241.130.127
   Admin status = Enabled, Operational status = Discovery,
   Weight = 1, Availability (%) = 0

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cluster</strong></td>
<td>The name of this Server Load Balancing (SLB) cluster.</td>
</tr>
<tr>
<td><strong>VIP</strong></td>
<td>The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>The classifier for the hypothetical packet, which can be L2 or L3.</td>
</tr>
<tr>
<td><strong>Admin status</strong></td>
<td>The current administrative status of this Server Load Balancing (SLB) cluster (Enabled or Disabled).</td>
</tr>
<tr>
<td><strong>Operational status</strong></td>
<td>The current operational status of this Server Load Balancing (SLB) cluster, which is In Service (at least one physical server is operational in the cluster) or Out of Service.</td>
</tr>
<tr>
<td><strong>Ping period (seconds)</strong></td>
<td>The ping period (in seconds) used by this Server Load Balancing (SLB) cluster to check the health of physical servers.</td>
</tr>
<tr>
<td><strong>Ping timeout (milliseconds)</strong></td>
<td>The timeout (in milliseconds) used by this Server Load Balancing (SLB) cluster to wait for ping answers from physical servers.</td>
</tr>
<tr>
<td><strong>Ping retries</strong></td>
<td>The number of ping retries that this Server Load Balancing (SLB) cluster executes before switching the status to No answer.</td>
</tr>
<tr>
<td><strong>Probe</strong></td>
<td>The probe configured for this cluster.</td>
</tr>
<tr>
<td><strong>Number of packets</strong></td>
<td>The number of packets balanced for this Server Load Balancing (SLB) cluster.</td>
</tr>
<tr>
<td><strong>Number of servers</strong></td>
<td>The total number of physical servers that belong to this Server Load Balancing (SLB) cluster.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td>The IP address for this physical server.</td>
</tr>
<tr>
<td><strong>Admin Status</strong></td>
<td>The administrative state of this physical server (Enabled or Disabled).</td>
</tr>
<tr>
<td><strong>Operational Status</strong></td>
<td>The operational state of this server. The possible states are described as follows:</td>
</tr>
<tr>
<td></td>
<td>- Disabled (this server is administratively disabled).</td>
</tr>
<tr>
<td></td>
<td>- No Answer (this server has not responded to ping requests).</td>
</tr>
<tr>
<td></td>
<td>- Link Down (there is a bad connection to this server).</td>
</tr>
<tr>
<td></td>
<td>- In Service (this server is used for SLB cluster client connections).</td>
</tr>
<tr>
<td></td>
<td>- Discovery (the SLB cluster is pinging this physical server).</td>
</tr>
<tr>
<td></td>
<td>- Retrying (the SLB cluster is making another attempt to bring up this server).</td>
</tr>
<tr>
<td><strong>Availability (%)</strong></td>
<td>The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.</td>
</tr>
</tbody>
</table>
-> show ip slb cluster Intranet statistics

<table>
<thead>
<tr>
<th>Cluster Name</th>
<th>Admin Status</th>
<th>Operational Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intranet</td>
<td>Enabled</td>
<td>In Service</td>
<td>3 Servers</td>
</tr>
<tr>
<td>Src IP 15.2.3.2/255.255.255.255</td>
<td></td>
<td>195</td>
<td></td>
</tr>
<tr>
<td>Src Port 1/4</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

- **Cluster Name**: The name of the SLB cluster. This field also contains the administrative and operational status for the cluster and either the VIP address or QoS policy condition value that identifies the cluster.

- **Admin status**: The current administrative status of this physical server (Enabled or Disabled).

- **Oper status**: The operational state of this server. The possible states are described as follows:
  - **Disabled** (this server is administratively disabled).
  - **No Answer** (this server has not responded to ping requests).
  - **Link Down** (there is a bad connection to this server).
  - **In Service** (this server is used for SLB cluster client connections).
  - **Discovery** (the SLB cluster is pinging this physical server).
  - **Retrying** (the SLB cluster is making another attempt to bring up this server).

- **Count**: The total number of physical servers that belong to the cluster, and the total number of packets serviced by the cluster.

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **ip slb reset statistics**: Resets SLB statistics for all clusters.
- **show ip slb clusters**: Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
- **show ip slb servers**: Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
- **show ip slb cluster server**: Displays detailed status and configuration information for a single physical server in a Server Load Balancing cluster.
- **ip slb cluster probe**: Configures a probe for an SLB cluster.
**MIB Objects**

slbClusterTable
   slbClusterName
   slbClusterVIP
   slbClusterAdminStatus
   slbClusterOperStatus
   slbClusterUpTime
   slbClusterPingPeriod
   slbClusterPingTimeout
   slbClusterPingRetries
   slbClusterRedirectAlgorithm
   slbClusterIdleTimer
   slbClusterNumberOfServers
   slbClusterProbeName
   slbClusterRowStatus
   slbClusterPackets
   slbClusterCondition
   slbClusterType

slbServerTable
   slbServerClusterName
   slbServerIpAddress
   slbServerAdminStatus
   slbServerOperStatus

slbStatsTable
   slbStatsClusterName
   slbStatsIndex
   slbStatsCounter

slbStatsQualTable
   slbStatsQualType
   slbStatsQualData
**show ip slb cluster server**

Displays detailed statistics and configuration information for a single physical server in a Server Load Balancing (SLB) cluster.

**show ip slb cluster name server ip_address**

---

**Syntax Definitions**

- **name**: Specifies the name of the SLB cluster.
- **ip_address**: Specifies the IP address for the physical server.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specifying a value for the *name* and *ip_address* parameters is required.

**Examples**

```bash
-> show ip slb cluster Intranet server 128.220.40.4
Cluster cl1
  VIP 128.220.40.205
  Server 128.220.40.4
    Admin status         : Enabled,
    Oper status          : In Service,
    Probe                = phttp,
    Availability time (%) = 95,
    Ping failures        = 0,
    Last ping round trip time (milliseconds) = 20
    Probe status         = ,
```

**output definitions**

- **Cluster**: The name of the Server Load Balancing (SLB) cluster.
- **VIP**: The virtual IP (VIP) address for this Server Load Balancing (SLB) cluster.
- **Server**: The IP address for this physical server.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin status</td>
<td>The current administrative status of this physical server (Enabled or Disabled).</td>
</tr>
<tr>
<td>Oper status</td>
<td>The operational state of this server. The possible states are described as follows:</td>
</tr>
<tr>
<td></td>
<td>• Disabled (this server is administratively disabled).</td>
</tr>
<tr>
<td></td>
<td>• No Answer (this server has not responded to ping requests).</td>
</tr>
<tr>
<td></td>
<td>• Link Down (there is a bad connection to this server).</td>
</tr>
<tr>
<td></td>
<td>• In Service (this server is used for SLB cluster client connections).</td>
</tr>
<tr>
<td></td>
<td>• Discovery (the SLB cluster is pinging this physical server).</td>
</tr>
<tr>
<td></td>
<td>• Retrying (the SLB cluster is making another attempt to bring up this server).</td>
</tr>
<tr>
<td>Probe</td>
<td>The name of the probe configured for this server.</td>
</tr>
<tr>
<td>Availability time (%)</td>
<td>The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.</td>
</tr>
<tr>
<td>Ping failures</td>
<td>The total number of pings that have failed on this physical server.</td>
</tr>
<tr>
<td>Last ping round trip time (milliseconds)</td>
<td>The total amount of time (in milliseconds) measured for the last valid ping to this physical server to make a round trip.</td>
</tr>
<tr>
<td>Probe status</td>
<td>The status of the probe configured for this server.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show ip slb servers` Displays the status of all physical servers belonging to Server Load Balancing clusters on a switch.
- `show ip slb clusters` Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
- `show ip slb cluster` Displays detailed status and configuration information for a single Server Load Balancing cluster.

**MIB Objects**

- `slbClusterTable`
  - `slbClusterVIP`
- `slbServerTable`
  - `slbServerClusterName`
  - `slbServerIpAddress`
  - `slbServerAdminStatus`
  - `slbServerOperStatus`
  - `slbServerMacAddress`
  - `slbServerSlotNumber`
  - `slbServerPortNumber`
  - `slbServerUpTime`
  - `slbServerProbeName`
  - `slbServerLastRTT`
<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>slbServerPingFails</td>
</tr>
<tr>
<td>slbServerProbeStatus</td>
</tr>
</tbody>
</table>
show ip slb servers

Displays the status and configurations of all physical servers in Server Load Balancing clusters.

show ip slb servers

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ip slb servers

+-----------------+----------------+----------+---------------+-----------
<table>
<thead>
<tr>
<th>IP addr</th>
<th>Cluster Name</th>
<th>Admin Status</th>
<th>Operational Status</th>
<th>Avail</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.220.40.4</td>
<td>Intranet</td>
<td>Enabled</td>
<td>In Service</td>
<td>98</td>
</tr>
<tr>
<td>128.220.40.5</td>
<td>Intranet</td>
<td>Enabled</td>
<td>Retrying</td>
<td>80</td>
</tr>
<tr>
<td>128.220.40.6</td>
<td>FileTransfer</td>
<td>Enabled</td>
<td>No answer</td>
<td>50</td>
</tr>
<tr>
<td>128.220.40.7</td>
<td>FileTransfer</td>
<td>Disabled</td>
<td>Disabled</td>
<td>---</td>
</tr>
<tr>
<td>128.220.40.1</td>
<td>WorldWideWeb</td>
<td>Enabled</td>
<td>In Service</td>
<td>100</td>
</tr>
<tr>
<td>128.220.40.2</td>
<td>WorldWideWeb</td>
<td>Enabled</td>
<td>Discovery</td>
<td>50</td>
</tr>
<tr>
<td>128.220.40.3</td>
<td>WorldWideWeb</td>
<td>Enabled</td>
<td>Link Down</td>
<td>75</td>
</tr>
</tbody>
</table>
```

**output definitions**

- **IP addr**: The IP address for this physical server.
- **Cluster Name**: The name of the Server Load Balancing (SLB) cluster to which this physical server belongs.
- **Admin Status**: The current administrative status of this physical server (**Enabled** or **Disabled**).
output definitions (continued)

<table>
<thead>
<tr>
<th>Operational Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>This server is administratively disabled.</td>
</tr>
<tr>
<td>No Answer</td>
<td>This server has not responded to ping requests.</td>
</tr>
<tr>
<td>Link Down</td>
<td>There is a bad connection to this server.</td>
</tr>
<tr>
<td>In Service</td>
<td>This server is used for SLB cluster client connections.</td>
</tr>
<tr>
<td>Discovery</td>
<td>The SLB cluster is pinging this physical server.</td>
</tr>
<tr>
<td>Retrying</td>
<td>The SLB cluster is making another attempt to bring up this server.</td>
</tr>
</tbody>
</table>

% Avail

The percentage of time that this physical server has been available for processing client requests. In other words, the actual ratio of up time (In Service plus Retrying) versus down time (No Answer plus Link Down). Please note that the Disabled and the initial Discovery states are not counted as down time.

Release History

Release 7.1.1; command introduced.

Related Commands

- **show ip slb cluster server**: Displays the detailed status and configuration of a single physical server in a Server Load Balancing cluster.
- **show ip slb clusters**: Displays detailed status and configuration information for all Server Load Balancing clusters on a switch.
- **show ip slb cluster**: Displays detailed status and configuration information for a single Server Load Balancing cluster.

MIB Objects

slbServers
  slbServerIpAddress
  slbServerClusterName
  slbServerAdminStatus
  slbServerOperStatus
  slbServerFlows
show ip slb probes

Displays the configuration of Server Load Balancing (SLB) probes.

show ip slb probes [probe_name]

Syntax Definitions

probe_name Specifies the name of the Server Load Balancing (SLB) probe.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you do not specify the name of an SLB probe then all SLB probes are displayed.

Examples

No probe name is specified:

-> show ip slb probes

<table>
<thead>
<tr>
<th>Probe Name</th>
<th>Period</th>
<th>Retries</th>
<th>Timeout</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>web_server</td>
<td>60000</td>
<td>3</td>
<td>12000</td>
<td>HTTP</td>
</tr>
<tr>
<td>mail_server</td>
<td>60000</td>
<td>3</td>
<td>3000</td>
<td>SMTP</td>
</tr>
<tr>
<td>mis_servers</td>
<td>360000</td>
<td>5</td>
<td>24000</td>
<td>Ping</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Probe Name</th>
<th>The user-specified name of the probe.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Period</td>
<td>The period (in seconds) to check the health of servers.</td>
</tr>
<tr>
<td>Retries</td>
<td>The number of probe retries before deciding that a server is out of service.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The timeout (in seconds) used to wait for probe answers.</td>
</tr>
<tr>
<td>Method</td>
<td>The type of probe.</td>
</tr>
</tbody>
</table>
The name of a probe that is not an HTTP/HTTPS probe is specified:

-> show ip slb probes mail_server

Probe mail_server
  Type = SMTP,
  Period (seconds) = 60,
  Timeout (milliseconds) = 3000,
  Retries = 3,
  Port = 0,

The name of an HTTP/HTTPS probe is specified:

-> show ip slb probes phttp

Probe phttp
  Type = HTTP,
  Period (seconds) = 60,
  Timeout (milliseconds) = 3000,
  Retries = 3,
  Port = 0,
  Username = ,
  Password = ,
  Expect = ,
  Status = 200,
  URL = /,

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe</td>
<td>The user-specified name of the probe.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of probe.</td>
</tr>
<tr>
<td>Period</td>
<td>The period (in seconds) to check the health of servers.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The timeout (in seconds) used to wait for probe answers.</td>
</tr>
<tr>
<td>Retries</td>
<td>The number of probe retries before deciding that a server is out of service.</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP/UDP port on which the probe is sent.</td>
</tr>
<tr>
<td>Username</td>
<td>The configured user name sent to a server as credentials for an HTTP GET operation for the probe.</td>
</tr>
<tr>
<td>Password</td>
<td>The configured password for the probe.</td>
</tr>
<tr>
<td>Expect</td>
<td>The configured ASCII string used to compare a response from a server to verify the health of the server.</td>
</tr>
<tr>
<td>Status</td>
<td>The expected status returned from an HTTP GET to verify the health of a server.</td>
</tr>
<tr>
<td>URL</td>
<td>The configured URL sent to a server for an HTTP GET to verify the health of the server.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- **ip slb probe**: Configures and deletes SLB probes.
- **ip slb probe period**: Configures the probe period to check the health of servers.
- **ip slb probe timeout**: Configures the timeout used to wait for probe answers.
- **ip slb probe retries**: Configures the number of probe retries before deciding that a server is out of service.
- **ip slb probe port**: Configures the TCP/UDP port that the probe should be sent on.
- **ip slb probe username**: Configures a user name sent to a server as credentials for an HTTP GET operation.
- **ip slb probe password**: Configures a password sent to a server as credentials for an HTTP GET to verify the health of the server.
- **ip slb probe expect**: Configures an ASCII string used to compare a response from a server to verify the health of the server.
- **ip slb probe status**: Configures the expected status returned from an HTTP GET to verify the health of a server.
- **ip slb probe url**: Configures a URL sent to a server for an HTTP GET to verify the health of the server.

**MIB Objects**

- slbProbeTable
  - slbProbeName
  - slbProbeMethod
  - slbProbePeriod
  - slbProbeTimeout
  - slbProbeRetries
  - slbProbePort
  - slbProbeHttpUsername
  - slbProbeHttpPassword
  - slbProbeExpect
  - slbProbeHttpStatus
  - slbProbeHttpUrl
32 IP Multicast Switching Commands

IP Multicast Switching (IPMS) is a one-to-many communication technique employed by emerging applications such as video distribution, news feeds, conferencing, netcasting, and resource discovery (OSPF, RIP2, and BOOTP). Unlike unicast, which sends one packet per destination, multicast sends one packet to all devices in any subnetwork that has at least one device requesting the multicast traffic.

The OmniSwitch IPMS software is compatible with the following RFCs:

- RFC 1112 — Host Extensions for IP Multicasting
- RFC 2236 — Internet Group Management Protocol, Version 2
- RFC 2933 — Internet Group Management Protocol MIB
- RFC 3376 — Internet Group Management Protocol, Version 3

The OmniSwitch IPv6MS software is compatible with the following RFCs:

- RFC 2710 — Multicast Listener Discovery for IPv6
- RFC 3019 — IPv6 MIB for Multicast Listener Discovery Protocol
- RFC 3810 — Multicast Listener Discovery Version 2 for IPv6

MIB information for the IPMS and IPv6MS commands is as follows:

Filename: ALCATEL-IND1-IPMS-MIB.mib
Module: alcatelIND1pmsMIB
The following table summarizes the available IP and IPv6 multicast commands:

<table>
<thead>
<tr>
<th>IP Multicast Command</th>
<th>IPv6 Multicast Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip multicast admin-state</td>
<td>ipv6 multicast admin-state</td>
</tr>
<tr>
<td>ip multicast flood-unknown</td>
<td>ipv6 multicast flood-unknown</td>
</tr>
<tr>
<td>ip multicast version</td>
<td>ipv6 multicast version</td>
</tr>
<tr>
<td>ip multicast port max-group</td>
<td>ipv6 multicast port max-group</td>
</tr>
<tr>
<td>ip multicast max-group</td>
<td>ipv6 multicast max-group</td>
</tr>
<tr>
<td>ip multicast static-neighbor</td>
<td>ipv6 multicast static-neighbor</td>
</tr>
<tr>
<td>ip multicast static-quicier</td>
<td>ipv6 multicast static-quicier</td>
</tr>
<tr>
<td>ip multicast static-group</td>
<td>ipv6 multicast static-group</td>
</tr>
<tr>
<td>ip multicast query-interval</td>
<td>ipv6 multicast query-interval</td>
</tr>
<tr>
<td>ip multicast last-member-query-interval</td>
<td>ipv6 multicast last-member-query-interval</td>
</tr>
<tr>
<td>ip multicast query-response-interval</td>
<td>ipv6 multicast query-response-interval</td>
</tr>
<tr>
<td>ip multicast unsolicited-report-interval</td>
<td>ipv6 multicast unsolicited-report-interval</td>
</tr>
<tr>
<td>ip multicast router-timeout</td>
<td>ipv6 multicast router-timeout</td>
</tr>
<tr>
<td>ip multicast source-timeout</td>
<td>ipv6 multicast source-timeout</td>
</tr>
<tr>
<td>ip multicast querying</td>
<td>ipv6 multicast querying</td>
</tr>
<tr>
<td>ip multicast robustness</td>
<td>ipv6 multicast robustness</td>
</tr>
<tr>
<td>ip multicast spoofing</td>
<td>ipv6 multicast spoofing</td>
</tr>
<tr>
<td>ip multicast spoofing static-source-ip</td>
<td>ipv6 multicast spoofing static-source-ip</td>
</tr>
<tr>
<td>ip multicast zapping</td>
<td>ipv6 multicast zapping</td>
</tr>
<tr>
<td>ip multicast querier-forwarding</td>
<td>ipv6 multicast querier-forwarding</td>
</tr>
<tr>
<td>ip multicast proxying</td>
<td>ipv6 multicast proxying</td>
</tr>
<tr>
<td>ip multicast helper-address</td>
<td>ipv6 multicast helper-address</td>
</tr>
<tr>
<td>ip multicast zero-based-query</td>
<td>ipv6 multicast zero-based-query</td>
</tr>
<tr>
<td>ip multicast forward-mode</td>
<td>ipv6 multicast forward-mode</td>
</tr>
<tr>
<td>ip multicast update-delay-interval</td>
<td>ipv6 multicast update-delay-interval</td>
</tr>
<tr>
<td>ip multicast fast-join</td>
<td>ipv6 multicast fast-join</td>
</tr>
<tr>
<td>ip multicast host-list</td>
<td>ipv6 multicast host-list</td>
</tr>
<tr>
<td>ip multicast ssm-map</td>
<td>ipv6 multicast ssm-map</td>
</tr>
<tr>
<td>ip multicast initial-packet-buffer admin-state</td>
<td>ipv6 multicast initial-packet-buffer admin-state,</td>
</tr>
<tr>
<td>ip multicast initial-packet-buffer max-packet</td>
<td>ipv6 multicast initial-packet-buffer max-packet</td>
</tr>
<tr>
<td>ip multicast initial-packet-buffer max-flow</td>
<td>ipv6 multicast initial-packet-buffer max-flow</td>
</tr>
<tr>
<td>ip multicast initial-packet-buffer timeout</td>
<td>ipv6 multicast initial-packet-buffer timeout</td>
</tr>
<tr>
<td>ip multicast initial-packet-buffer min-delay</td>
<td>ipv6 multicast initial-packet-buffer min-delay</td>
</tr>
<tr>
<td>ip multicast display-interface-names</td>
<td>ipv6 multicast display-interface-names</td>
</tr>
<tr>
<td>ip multicast inherit-default-vrf-config</td>
<td>ipv6 multicast inherit-default-vrf-config</td>
</tr>
<tr>
<td>ip multicast profile</td>
<td>ipv6 multicast profile</td>
</tr>
<tr>
<td>ip multicast apply-profile</td>
<td>ipv6 multicast apply-profile</td>
</tr>
<tr>
<td>show ip multicast</td>
<td>show ipv6 multicast</td>
</tr>
<tr>
<td>show ip multicast port</td>
<td>show ipv6 multicast port</td>
</tr>
<tr>
<td>show ip multicast forward</td>
<td>show ipv6 multicast forward</td>
</tr>
<tr>
<td>show ip multicast neighbor</td>
<td>show ipv6 multicast neighbor</td>
</tr>
<tr>
<td>show ip multicast querier</td>
<td>show ipv6 multicast querier</td>
</tr>
<tr>
<td>show ip multicast group</td>
<td>show ipv6 multicast group</td>
</tr>
<tr>
<td>show ip multicast source</td>
<td>show ipv6 multicast source</td>
</tr>
<tr>
<td>show ip multicast tunnel</td>
<td>show ipv6 multicast tunnel</td>
</tr>
<tr>
<td>show ip multicast host-list</td>
<td>show ipv6 multicast host-list</td>
</tr>
<tr>
<td>show ip multicast ssm-map</td>
<td>show ipv6 multicast ssm-map</td>
</tr>
<tr>
<td>show ip multicast bridge</td>
<td>show ipv6 multicast bridge</td>
</tr>
<tr>
<td>show ip multicast bridge-forward</td>
<td>show ipv6 multicast bridge-forward</td>
</tr>
<tr>
<td>show ip multicast bidir-forward</td>
<td>show ipv6 multicast bidir-forward</td>
</tr>
<tr>
<td>show ip multicast profile</td>
<td>show ipv6 multicast profile</td>
</tr>
</tbody>
</table>
ip multicast admin-state

Enables or disables IP Multicast Switching and Routing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] admin-state [enable | disable]

no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] admin-state

Syntax Definitions

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **service_id[-service_id2]**: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*
- **enable**: Enable IP Multicast Switching.
- **disable**: Disable IP Multicast Switching.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The configuration of an IP multicast routing protocol on an IP interface operationally triggers IP Multicast Switching and Routing functionality on any underlying VLAN or SPB service. This occurs regardless of any explicit IPMS configuration, such as attempting to specifically disable IPMS.

- If there is no IP Multicast routing protocol already running on the switch, then the **ip multicast admin-state** or the **ipv6 multicast admin-state** command alone controls IPMS operations.

- Enabling IPMS on individual VLANs or services, as needed, is recommended to conserve switch resources.
- If IPMS is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

**Note.** Globally enabling the IPMS status for the switch only applies to the VLAN domain (does not apply to the service domain). As a result, IPMS must be explicitly enabled or disabled for each SPB service. However, globally disabling IPMS for all SPB services is supported.

- Use the `no` form of this command to restore the IP Multicast Switching and Routing status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

**Examples**

-> ip multicast admin-state enable
-> ip multicast admin-state disable
-> no ip multicast admin-state
-> ip multicast vlan 2 admin-state enable
-> ip multicast vlan 3-5 admin-state disable
-> no ip multicast vlan 2 admin-state
-> no ip multicast vlan 3-5 admin-state
-> ip multicast service 10 admin-state enable
-> ip multicast service 11-15 admin-state disable
-> no ip multicast service 10 admin-state
-> no ip multicast service 11-15 admin-state

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

- `show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigStatus
ip multicast flood-unknown

Enables or disables the flooding unknown multicast traffic for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified. When a traffic flow is first seen on a port, there is a brief period of time where traffic may get dropped before the forwarding information is calculated. When flooding unknown multicast traffic is enabled, no packets are dropped before the forwarding information is available.

```
ip multicast [vlan vlan_id][-vlan_id2] | service service_id[-service_id2] flood-unknown [enable | disable]
no ip multicast [vlan vlan_id][-vlan_id2] | service service_id[-service_id2] flood-unknown
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable` Enable flooding of unknown traffic until it is learned.
- `disable` Disable flooding of unknown traffic.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If this command function is enabled after the system is up and running, the flooding of unknown multicast traffic only applies to new flows.
- If the flooding of unknown traffic is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
On an OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900:

- The flood unknown behavior configured for any VLAN is enforced only on that VLAN. However, when the behavior is configured with the IPv6 multicast version of this command (ipv6 multicast flood-unknown) for any VLAN, the flood unknown behavior is enforced globally across all VLANs.
- IPv4 multicast snooping for VLANs does not snoop 224.0.0.0/24 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded IPv4 addresses.
- When IPv4 multicast snooping is enabled for any service, the flooding of unknown multicast traffic is unconditionally enforced for all snooping services; this is the only supported flood unknown behavior for services.
- IPv4 multicast snooping for services does not snoop MAC addresses that fall within the range of 01:00:5e:00:00:00/40 and 33:33:00:00:00:00/40 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded MAC addresses.

On an OmniSwitch 9900, IPv4 multicast snooping for VLANs or services does not snoop 224.0.0.0/24 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to these excluded IPv4 addresses.

- Use this command to provide an "open failure" strategy for when hardware resource conflicts or software limits prevent the traffic from being registered in the fast path.
- Use the no form of this command to restore the flooding of unknown traffic back to the default value (disabled) on the system or the specified VLAN.

**Examples**

```plaintext
-> ip multicast flood-unknown enable
-> ip multicast flood-unknown disable
-> no ip multicast flood-unknown
-> ip multicast vlan 100 flood-unknown enable
-> ip multicast vlan 101-105 flood-unknown enable
-> ip multicast vlan 100 flood-unknown disable
-> no ip multicast vlan 100 flood-unknown
-> no ip multicast vlan 101-105 flood-unknown
-> ip multicast service 10 flood-unknown enable
-> ip multicast service 11-15 flood-unknown enable
-> ip multicast service 10 flood-unknown disable
-> no ip multicast service 10 flood-unknown
-> no ip multicast service 11-15 flood-unknown
```

**Release History**

Release 8.3.1; command introduced.
Release 8.4.1.R02; service parameter added.
Related Commands

**show ip multicast**  Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigFloodUnknown
**ip multicast version**

Sets the default version of the IGMP protocol on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] version [version]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] version
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `version` Default IGMP protocol version to run. Valid range is 1–3.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>2</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IP Multicast Switching and Routing must be enabled to set the default IGMP protocol version on the system and/or the specified VLANs or SPB services.
- If the default IGMP protocol version is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Due to protocol inter-operation requirements, this command specifies only a default version of the IGMP protocol to run.
- Use the **no** form of this command to restore the IGMP multicast version back to the default value (version 2) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, `ip multicast version 0`).
**Examples**

-> ip multicast version 3  
-> ip multicast version 0  
-> no ip multicast version  
-> ip multicast vlan 2 version 3  
-> ip multicast vlan 3-5 version 3  
-> ip multicast vlan 2 version 0  
-> no ip multicast vlan 2 version  
-> no ip multicast vlan 3-5 version  
-> ip multicast service 2 version 3  
-> ip multicast service 3-5 version 3  
-> ip multicast service 2 version 0  
-> no ip multicast service 2 version  
-> no ip multicast service 3-5 version

**Release History**

Release 7.1.1; command was introduced.  
Release 8.4.1; service parameter added.

**Related Commands**

**show ip multicast** Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigType  
  alaIpmsConfigAddressType  
  alaIpmsConfigValue  
  alaIpmsConfigVersion
**ip multicast port max-group**

Configures the maximum group limit learned per port or per Service Access Point (SAP) port. The group limit is applicable to all VLAN instances associated with the specified port or all Shortest Path Bridging (SPB) service instances associated with the specified SAP port.

```
ip multicast {port chassis/slot/port | sap port sap_id} max-group [num] [action {none | drop | replace}]
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.
- **slot/port**
  - The slot and port number (3/1).
- **sap_id**
  - The SAP ID (chassis/slot/port:encapsulation). *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **num**
  - The maximum IGMP group count. Valid range is 0–4294967295.
- **none**
  - Disables the maximum group limit configuration.
- **drop**
  - Drops the incoming membership request.
- **replace**
  - Replaces an existing membership with the incoming membership request. A leave is not sent to the router for the replaced group.

### Defaults

By default, the maximum group limit is set to zero.

<table>
<thead>
<tr>
<th>parameter</th>
<th>defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If group memberships are already registered on a port/VLAN or SAP port/SPB service instance and the group limit is set to a lower value for the instance, the current group memberships are not removed until they expire. The effect of the new lower group limit value is applied when one of the following occurs to help avoid any undetermined behavior:
  - IP multicast memberships are aged out on a port/VLAN or SAP port/SPB service instance.
  - IP multicast memberships are pruned by a leave or when IP multicast is disabled on the specific VLAN or SPB service or globally disabled for the switch.
• If the `num` and `action` parameters are not specified, then the limit is removed.

• When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ip multicast sap port 1/1/23:10 max-group 10 action drop`, where 1/1/23:10 is the SAP ID).

• A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

• IGMP zapping must be enabled when the maximum group limit is enabled and the action is set to drop.

• Configuring a maximum group limit is allowed even when the IP multicast status is disabled.

• The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
  – Group limit configured for a port or an SPB SAP port.
  – Group limit configured for a specific VLAN or SPB service.
  – Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
  – Group limit configured for a VLAN or SPB service within a specific VRF context.
  – Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.

**Examples**

```
-> ip multicast port 1/1/12 max-group 10 action drop
-> ip multicast port 1/1/14 max-group 20 action replace
-> ip multicast port 1/1/14 max-group

-> ip multicast sap port 1/1/23:10 max-group 10 action drop
-> ip multicast sap port 1/1/26:20.200 max-group 20 action replace
-> ip multicast sap port 1/1/16:20.200 max-group
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `sap port` parameter added.

**Related Commands**

- `show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.
- `show ip multicast port` Displays the maximum group configuration for VLAN ports or SPB service SAP ports.

**MIB Objects**

- `alaIpmsIntfTable` `alaIpmsIntfConfigType` `alaIpmsIntfAddressType` `alaIpmsIntfMaxGroupLimit` `alaIpmsIntfMaxGroupExceedAction`
**ip multicast max-group**

Configures the maximum group limit learned per port for the specified VLAN, Shortest Path Bridging (SPB) service, or per port on the system if no VLAN or SPB service is specified. The limit is applied to each port that is a member of the given VLAN or SPB service and the specified action is taken when the limit is exceeded.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] max-group [num] [action {none | drop | replace}]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `num` The maximum IGMP group count. Valid range is 0–4294967295.
- `none` Disables the maximum group limit configuration.
- `drop` Drops the incoming membership request.
- `replace` Replaces an existing membership with the incoming membership request.

**Defaults**

By default, the maximum group limit is set to zero.

<table>
<thead>
<tr>
<th>parameter</th>
<th>defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a VLAN or SPB service is not specified, this command configures the global maximum group limit applied to all VLAN ports and SPB Service Access Point (SAP) ports.
- If a VLAN is specified, this command configures the maximum group limit learned per port on a VLAN. The limit is applied to each port that is a member of the given VLAN.
• If an SPB service is specified, this command configures the maximum group limit learned per SAP port on a service. The limit is applied to each SAP port that is a member of the given SPB service.

• Configuring a maximum group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN or SAP port/SPB service instance

• If the num and action parameters are not specified, then the limit is removed.

• The maximum group configuration on a VLAN or SPB service will override the global configuration.

• The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
  – Group limit configured for a port or an SPB SAP port.
  – Group limit configured for a specific VLAN or SPB service.
  – Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
  – Group limit configured for a VLAN or SPB service within a specific VRF context.
  – Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.

• IGMP zapping must be enabled when the maximum group limit is enabled and the action is to drop incoming membership requests.

**Examples**

```
-> ip multicast max-group 10 action drop
-> ip multicast max-group 20 action replace
-> ip multicast max-group
-> ip multicast vlan 10 max-group 10 action drop
-> ip multicast vlan 20 max-group action drop
-> ip multicast vlan 11-15 max-group 10 action replace
-> ip multicast vlan 10 max-group
-> ip multicast vlan 11-15 max-group
-> ip multicast service 5 max-group 10 action drop
-> ip multicast service 20 max-group action drop
-> ip multicast service 10-15 max-group 10 action replace
-> ip multicast service 5 max-group
-> ip multicast service 10-15 max-group
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; service parameter added.
Related Commands

**show ip multicast**  
Displays the IP Multicast Switching and Routing status and general configuration parameters.

**show ip multicast group**  
Displays the maximum group configuration for all port or VLAN instances of a given port or all ports.

MIB Objects

alaIpmsConfigTable
  alaIpmsConfigType  
  alaIpmsConfigAddressType  
  alaIpmsConfigValue  
  alaIpmsConfigMaxGroupLimit  
  alaIpmsConfigMaxGroupExceedAction
**ip multicast static-neighbor**

Creates a static IGMP neighbor entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

```plaintext
ip multicast static-neighbor vlan vlan_id {port chassis/slot/port | linkagg agg_id}
ip multicast static-neighbor service service_id sap {port | linkagg} {sap_id}
no ip multicast static-neighbor vlan vlan_id {port chassis/slot/port | linkagg agg_id}
no ip multicast static-neighbor service service_id sap {port | linkagg} {sap_id}
```

**Syntax Definitions**

- `vlan_id`: VLAN to include as a static IGMP neighbor.
- `chassis`: The chassis identifier.
- `slot/port`: The slot and port number to configure as a static IGMP neighbor.
- `agg_id`: The link aggregate ID number to configure as a static IGMP neighbor.
- `service_id`: SPB service ID to include as a static IGMP neighbor. The valid range is 1–32767. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `sap_id`: The SAP ID (chassis/slot/port:encapsulation). This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an IGMP static neighbor entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an IGMP static neighbor entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the IGMP traffic and IPv4 multicast traffic.
- To create an IGMP static neighbor entry on a link aggregate, use the `linkagg` parameter (for example, `ip multicast static-neighbor vlan 2 linkagg 7` or `ip multicast static-neighbor service 10 sap linkagg 10:100`).
- When using the sap port parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ip multicast static-neighbor service 10 sap port 1/1/23:10`, where 1/1/23:10 is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

### Examples

```
-> ip multicast static-neighbor vlan 4 port 1/1/5
-> no ip multicast static-neighbor vlan 4 port 1/1/5
-> ip multicast static-neighbor vlan 4 linkagg 7
-> no ip multicast static-neighbor vlan 4 linkagg 7

-> ip multicast static-neighbor service 10 sap port 1/1/2:100
-> no ip multicast static-neighbor service 10 sap port 1/1/2:100
-> ip multicast static-neighbor service 10 sap linkagg 10:100
-> no ip multicast static-neighbor service 10 sap linkagg 10:100
```

### Release History

Release 7.1.1; command was introduced.
Release 7.3.1; **linkagg** parameter was introduced.
Release 8.4.1; **service** and **sap** parameters added.

### Related Commands

- **show ip multicast neighbor** Displays the IGMP neighbor table entries of IP Multicast Switching and Routing.

### MIB Objects

- `alaIpmsStaticNeighborTable`
  - `alaIpmsStaticNeighborConfigType`
  - `alaIpmsStaticNeighborAddressType`
  - `alaIpmsStaticNeighborValue`
  - `alaIpmsStaticNeighborIfIndex`
  - `alaIpmsStaticNeighborSubValue`
  - `alaIpmsStaticNeighborRowStatus`
ip multicast static-querier

Creates a static IGMP querier entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

Syntax:
ip multicast static-querier vlan vlan_id {port chassis/slot/port | linkagg agg_id}  
ip multicast static-querier service service_id sap {port | linkagg} {sap_id}  
no ip multicast static-querier vlan vlan_id {port chassis/slot/port | linkagg agg_id}  
no ip multicast static-querier service service_id sap {port | linkagg} {sap_id}

Syntax Definitions:

- **vlan_id**: VLAN to include as a static IGMP querier.
- **chassis**: The chassis identifier.
- **slot|port**: The slot and port number to configure as a static IGMP querier.
- **agg_id**: The link aggregate ID number to configure as a static IGMP querier.
- **service_id**: SPB service ID to include as a static IGMP querier. The valid range is 1–32767. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- **sap_id**: The SAP ID (chassis/slot/port:encapsulation). This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.

Defaults:

N/A

Platforms Supported:

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines:

- Use the no form of this command to remove an IGMP static querier entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.

- Creating an IGMP static querier entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the IGMP traffic.

- To create an IGMP static querier entry on a link aggregate, use the linkagg parameter (for example, ip multicast static-querier vlan 2 linkagg 7 or ip multicast static-querier service 10 sap linkagg 10:100).
When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ip multicast static-querier service 10 sap port 1/1/23:10`, where 1/1/23:10 is the SAP ID).

A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

**Examples**

```
-> ip multicast static-querier vlan 4 port 1/1/2
-> no ip multicast static-querier vlan 4 port 1/1/2
-> ip multicast static-querier vlan 4 linkagg 7
-> no ip multicast static-querier vlan 4 linkagg 7

-> ip multicast static-querier service 10 sap port 1/1/2:100
-> no ip multicast static-querier service 10 sap port 1/1/2:100
-> ip multicast static-querier service 10 sap linkagg 10:100
-> no ip multicast static-querier service 10 sap linkagg 10:100
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.1; `linkagg` parameter was added.
Release 8.4.1; `service` and `sap` parameters added.

**Related Commands**

`show ip multicast querier` Displays the IGMP querier table entries of IP Multicast Switching and Routing.

**MIB Objects**

- `alaIpmsStaticQuerierTable`
  - `alaIpmsStaticQuerierConfigType`
  - `alaIpmsStaticQuerierAddressType`
  - `alaIpmsStaticQuerierValue`
  - `alaIpmsStaticQuerierIfIndex`
  - `alaIpmsStaticQuerierSubValue`
  - `alaIpmsStaticQuerierRowStatus`
**ip multicast static-group**

Creates a static IGMP group entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

```plaintext
ip multicast static-group ip_address vlan vlan_id {port chassis/slot/port | linkagg agg_id}
ip multicast static-group ip_address service service_id sap {port | linkagg} {sap_id}
no ip multicast static-group ip_address vlan vlan_id {port chassis/slot/port | linkagg agg_id}
no ip multicast static-group ip_address service service_id sap {port | linkagg} {sap_id}
```

**Syntax Definitions**

- **ip_address**
  - The IP address of the multicast group.

- **vlan_id**
  - VLAN to include as a static IGMP group.

- **chassis**
  - The chassis identifier.

- **slot|port**
  - The slot and port number to configure as a static IGMP group.

- **agg_id**
  - The link aggregate ID number to configure as a static IGMP group.

- **service_id**
  - SPB service ID to include as a static IGMP group. The valid range is 1–32767. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

- **sap_id**
  - The SAP ID (chassis/slot/port:encapsulation). *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an IGMP static group entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.

- Creating an IGMP static group entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive IGMP traffic addressed to the specified IP multicast group address.
To create an IGMP static group entry on a link aggregate, use the `linkagg` parameter (for example, `ip multicast static-group 225.0.0.1 vlan 2 linkagg 7` or `ip multicast static-group 225.0.0.1 service 10 sap linkagg 10:100`).

When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ip multicast static-ququerier service 10 sap port 1/1/23:10`).

A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

**Examples**

```
-> ip multicast static-group 229.10.10.10 vlan 4 port 1/1/2  
-> no ip multicast static-group 229.10.10.10 vlan 4 port 1/1/2 
-> ip multicast static-group 225.11.11.11 vlan 4 linkagg 7  
-> no ip multicast static-group 225.11.11.11 vlan 4 linkagg 7 

-> ip multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100 
-> no ip multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100 
-> ip multicast static-group 225.11.11.11 service 10 sap linkagg 10:100  
-> no ip multicast static-group 225.11.11.11 service 10 sap linkagg 10:100 
```

**Release History**

Release 7.1.1; command was introduced.  
Release 7.3.1; `linkagg` parameter was added.  
Release 8.4.1; `service` and `sap` parameters added.

**Related Commands**

- `show ip multicast group` Displays the IGMP group membership table entries of IP Multicast Switching and Routing for the specified IP multicast group address or all entries if no IP multicast group address is specified.

**MIB Objects**

alaIgmpStaticMemberTable
  `alaIgmpStaticMemberConfigType`  
  `alaIgmpStaticMemberAddressType`  
  `alaIgmpStaticMemberValue`  
  `alaIgmpStaticMemberIfIndex`  
  `alaIgmpStaticMemberSubValue`  
  `alaIgmpStaticMemberGroupAddress`  
  `alaIgmpStaticMemberRowStatus`
**ip multicast query-interval**

Sets the IGMP query interval on the specified VLAN, Shortest Path Bridging (SPB), or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2] query-interval [seconds]
```

```
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2] query-interval
```

### Syntax Definitions

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **service_id[-service_id2]**: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*
- **seconds**: IGMP query interval in seconds. Valid range is 1–65535.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>125</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP query interval on the system and/or the specified VLANs or SPB services.
- If the IGMP query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The IGMP query interval refers to the time period between IGMP query messages.
- Due to protocol inter-operation requirements, this command specifies only a default version of the IGMP query interval to use.
- Use the **no** form of this command to restore the IGMP query interval back to the default value (125 seconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a
value of 0 with this command also restores the default value (for example, `ip multicast query-interval 0`).

**Examples**

-> `ip multicast query-interval 100`
-> `ip multicast query-interval 0`
-> `no ip multicast query-interval`
-> `ip multicast vlan 2 query-interval 100`
-> `ip multicast vlan 3-5 query-interval 100`
-> `ip multicast vlan 2 query-interval 0`
-> `no ip multicast vlan 2 query-interval`
-> `no ip multicast vlan 3-5 query-interval`
-> `ip multicast service 2 query-interval 100`
-> `ip multicast service 3-5 query-interval 100`
-> `ip multicast service 2 query-interval 0`
-> `no ip multicast service 2 query-interval`
-> `no ip multicast service 3-5 query-interval`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

`show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigQueryInterval
**ip multicast last-member-query-interval**

Sets the IGMP last member query interval value on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] last-member-query-interval [tenths_of_seconds]
```

```
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] last-member-query-interval
```

**Syntax Definitions**

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **service_id[-service_id2]**: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **tenths_of_seconds**: IGMP last member query interval in tenths of seconds. The valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>tenths_of_seconds</strong></td>
<td>10</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IP Multicast Switching and Routing must be enabled to set the IGMP last member query interval on the system and/or the specified VLANs or SPB services.
- If the IGMP last member query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The IGMP last member query interval refers to the time period to reply to an IGMP query message sent in response to a leave group message.
- Use the **no** form of this command to restore the IGMP last member query interval back to the default value (10 tenths-of-seconds) on the system, the specified VLAN, or the specified SPB service. In
addition, specifying a value of 0 with this command also restores the default value (for example, `ip multicast last-member-query-interval 0`).

**Examples**

```
-> ip multicast last-member-query-interval 22
-> ip multicast last-member-query-interval 0
-> no ip multicast last-member-query-interval
-> ip multicast vlan 2 last-member-query-interval 22
-> ip multicast vlan 3-5 last-member-query-interval 22
-> ip multicast vlan 2 last-member-query-interval 0
-> no ip multicast vlan 2 last-member-query-interval
-> no ip multicast vlan 3-5 last-member-query-interval
-> ip multicast service 2 last-member-query-interval 22
-> ip multicast service 3-5 last-member-query-interval 22
-> ip multicast service 2 last-member-query-interval 0
-> no ip multicast service 2 last-member-query-interval
-> no ip multicast service 3-5 last-member-query-interval
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

- `show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigLastMemberQueryInterval`
**ip multicast query-response-interval**

Sets the IGMP query response interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
```

```
oip multicast [vlan vlan_id[-vlan_id2] | service service_id] query-response-interval
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` : VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` : SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `tenths_of_seconds` : IGMP query response interval in tenths of seconds. The valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>tenths_of_seconds</code></td>
<td>100</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IP Multicast Switching and Routing must be enabled to set the IGMP query response interval on the system and/or the specified VLANs or SPB services.
- If the IGMP query response interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The query response interval refers to the time period to reply to an IGMP query message.
- Use the `no` form of this command to restore the IGMP query response interval back to the default value (100 tenths-of-seconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, `ip multicast query-response-interval 0`).
**Examples**

- `ip multicast query-response-interval 200`
- `ip multicast query-response-interval 0`
- `no ip multicast query-response-interval`
- `ip multicast vlan 2 query-response-interval 300`
- `ip multicast vlan 3-5 query-response-interval 300`
- `no ip multicast vlan 2 query-response-interval 0`
- `ip multicast vlan 2 query-response-interval 0`
- `no ip multicast vlan 2 query-response-interval 0`
- `ip multicast service 2 query-response-interval 300`
- `ip multicast service 3-5 query-response-interval 300`
- `ip multicast service 2 query-response-interval 0`
- `no ip multicast service 2 query-response-interval`
- `no ip multicast service 3-5 query-response-interval`
- `no ip multicast service 2 query-response-interval`
- `no ip multicast service 3-5 query-response-interval`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; service parameter added.

**Related Commands**

- `show ip multicast`
  Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigQueryResponseInterval`
**ip multicast unsolicited-report-interval**

Sets the value of the IGMP unsolicited report interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] unsolicited-report-interval [seconds]
```

```
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] unsolicited-report-interval
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `seconds` IGMP unsolicited report interval in seconds. Valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IP Multicast Switching and Routing must be enabled to set the IGMP unsolicited report interval on the system and/or the specified VLANs or SPB services.
- If the IGMP query response interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The unsolicited report interval refers to the time period to proxy any changed IGMP membership state.
- Use the `no` form of this command to restore the IGMP unsolicited report interval back to the default value (1 second) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, `ip multicast unsolicited-report-interval 0`).
**Examples**

- `ip multicast unsolicited-report-interval 200`
- `ip multicast unsolicited-report-interval 0`
- `no ip multicast unsolicited-report-interval`
- `ip multicast vlan 2 unsolicited-report-interval 300`
- `ip multicast vlan 3-5 unsolicited-report-interval 300`
- `ip multicast vlan 2 unsolicited-report-interval 0`
- `no ip multicast vlan 2 unsolicited-report-interval`
- `ip multicast service 2 unsolicited-report-interval 300`
- `ip multicast service 3-5 unsolicited-report-interval 300`
- `ip multicast service 2 unsolicited-report-interval 0`
- `no ip multicast service 2 unsolicited-report-interval`
- `no ip multicast service 3-5 unsolicited-report-interval`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

`show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

`alaIpmsConfigTable`  
`alaIpmsConfigType`  
`alaIpmsConfigAddressType`  
`alaIpmsConfigValue`  
`alaIpmsConfigUnsolicitedReportInterval`
**ip multicast router-timeout**

Configures the expiry time of IP multicast routers on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```bash
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] router-timeout [seconds]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] router-timeout
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `seconds` IGMP router timeout in seconds. Valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>90</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IP Multicast Switching and Routing must be enabled to set the IGMP router timeout on the system and/or the specified VLANs.

- If the IGMP router timeout is already configured on the system, then the VLAN configuration will override the system's configuration.

- Use the `no` form of this command to restore the IGMP router timeout back to the default value (90 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, `ip multicast router-timeout 0`).

**Examples**

```bash
-> ip multicast router-timeout 100
-> ip multicast router-timeout 0
```
-> no ip multicast router-timeout
-> ip multicast vlan 2 router-timeout 100
-> ip multicast vlan 3-5 router-timeout 100
-> ip multicast vlan 2 router-timeout 0
-> no ip multicast vlan 2 router-timeout
-> no ip multicast vlan 3-5 router-timeout
-> ip multicast service 2 router-timeout 100
-> ip multicast service 3-5 router-timeout 100
-> ip multicast service 2 router-timeout 0
-> no ip multicast service 2 router-timeout
-> no ip multicast servicee 3-5 router-timeout

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R02; service parameter added.

**Related Commands**

*show ip multicast* Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigRouterTimeout
ip multicast source-timeout

Configures the expiry time of IP multicast sources on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] source-timeout [seconds]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] source-timeout
```

**Syntax Definitions**

- `vlan [vlan_id][-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service [service_id][-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `seconds`: IGMP source timeout in seconds. Valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>30</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IP Multicast Switching and Routing must be enabled to set the IGMP source timeout on the system and/or the specified VLANs.
- If the IGMP source timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- Use the `no` form of this command to restore the IGMP source timeout back to the default value (30 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, `ip multicast source-timeout 0`).

**Examples**

```
-> ip multicast source-timeout 100
-> ip multicast source-timeout 0
```
-> no ip multicast source-timeout
-> ip multicast vlan 2 source-timeout 100
-> ip multicast vlan 3-5 source-timeout 100
-> ip multicast vlan 2 source-timeout 0
-> no ip multicast vlan 2 source-timeout
-> no ip multicast vlan 3-5 source-timeout 100
-> ip multicast service 2 source-timeout 100
-> ip multicast service 3-5 source-timeout 100
-> ip multicast service 2 source-timeout 0
-> no ip multicast service 2 source-timeout
-> no ip multicast service 3-5 source-timeout

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R02; service parameter added.

**Related Commands**

`show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigSourceTimeout
ip multicast querying

Enables or disables IGMP querying on the specified VLAN or on the system if no VLAN is specified.

```
ip multicast [vlan vlan_id[-vlan_id2]] querying {enable | disable} [static-source-ip ip_address]
no ip multicast [vlan vlan_id[-vlan_id2]] querying [static-source-ip]
```

### Syntax Definitions

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `enable` Enable IGMP querying.
- `disable` Disable IGMP querying.
- `ip_address` A static source IPv4 address to use for IGMP querying. This parameter is not supported.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- IP Multicast Switching and Routing must be enabled to enable IGMP querying on the system and/or specified VLANs.
- If the IGMP querying is already enabled/disabled on the system, then the VLAN configuration will override the system's configuration.
- IGMP querying refers to requesting the network's IGMP group membership information by sending out IGMP queries. IGMP querying also involves participating in IGMP querier election.
- Use the `no` form of this command to restore the IGMP querying status to the default value (disabled) on the system or the specified VLAN.

### Examples

```
-> ip multicast querying enable
-> ip multicast querying disable
```
-> no ip multicast querying
-> ip multicast vlan 2 querying enable
-> ip multicast vlan 3-5 querying disable
-> no ip multicast vlan 2 querying
-> no ip multicast vlan 3-5 querying

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1.R02; **static-source-ip** parameter added.

**Related Commands**

**show ip multicast**

Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigQuerying
  alaIpmsConfigQueryingStaticSourceAddress
ip multicast robustness

Sets the IGMP robustness variable on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] robustness [robustness]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] robustness
```

Syntax Definitions

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `robustness`: IGMP robustness variable. Valid range is 1–7.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>robustness</td>
<td>2</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- IP Multicast Switching and Routing must be enabled to set the IGMP robustness variable on the system and/or the specified VLANs or SPB services.
- If the IGMP robustness variable is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Robustness variable allows fine-tuning on the network, where the expected packet loss would be greater.
- Due to protocol inter-operation requirements, this command specifies only a default version of the IGMP robustness variable to use.
Use the **no** form of this command to restore the IGMP robustness variable back to the default value (2) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, ip multicast robustness 0).

### Examples

```
-> ip multicast robustness 3
-> ip multicast robustness 0
-> no ip multicast robustness
-> ip multicast vlan 2 robustness 3
-> ip multicast vlan 3-5 robustness 3
-> ip multicast vlan 2 robustness 0
-> no ip multicast vlan 2 robustness
-> no ip multicast vlan 3-5 robustness
-> ip multicast service 2 robustness 3
-> ip multicast service 3-5 robustness 3
-> ip multicast service 2 robustness 0
-> no ip multicast service 2 robustness
-> no ip multicast service 3-5 robustness
```

### Release History

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

### Related Commands

- **show ip multicast**  
  Displays the IP Multicast Switching and Routing status and general configuration parameters.

### MIB Objects

- **alaIpmsConfigTable**
  - **alaIpmsConfigType**
  - **alaIpmsConfigAddressType**
  - **alaIpmsConfigValue**
  - **alaIpmsConfigRobustness**
**ip multicast spoofing**

Enables or disables IGMP spoofing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing {enable | disable}
```

```
oip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable`: Enable IGMP spoofing.
- `disable`: Disable IGMP spoofing.

** Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an IGMP spoofing configuration and return the specified VLAN, SPB service, or system to the default behavior.
- If the IGMP spoofing is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- IGMP spoofing refers to replacing a client source MAC and IP address with the system's MAC and IP address when relaying or proxying aggregated IGMP group membership information to other devices.
- By default, the source IP address is not specified for spoofing; the system determines these addresses automatically. Optionally configure a static source IP address using the `ip multicast spoofing static-source-ip` command to overcome the need for an IP interface. If configured, the static source IP is always used for spoofing, regardless of the IP interface address or administrative state.
Examples

- `ip multicast spoofing enable`
- `ip multicast spoofing disable`
- `no ip multicast spoofing`
- `ip multicast vlan 2 spoofing enable`
- `ip multicast vlan 3-5 spoofing disable`
- `no ip multicast vlan 2 spoofing`
- `no ip multicast vlan 3-5 spoofing`
- `ip multicast service 2 spoofing enable`
- `ip multicast service 3-5 spoofing disable`
- `no ip multicast service 2 spoofing`
- `no ip multicast service 3-5 spoofing`

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; service parameter added.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigSpoofing
**ip multicast spoofing static-source-ip**

Configures an IGMP static spoofing address on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing static-source-ip ip_address
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing static-source-ip
```

### Syntax Definitions

- **vlan_id[-vlan_id2]**  
  VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.

- **service_id[-service_id2]**  
  SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

- **ip_address**  
  A static source IPv4 address to use for spoofing.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove a static source IP address.

- IGMP spoofing refers to replacing a client source MAC and IP address with the system's MAC and IP address when relaying or proxying aggregated IGMP group membership information to other devices.

- By default, a source IP address is not specified when spoofing is enabled. As a result, the switch will automatically use the address of the IP interface associated with the LAN. If there is no IP interface address to use, the switch will then use the Loopback0 interface address associated with the current VRF instance.

- Use this command to optionally configure a static source IP address to overcome the need for an IP interface. If configured, the static source IP is always used for spoofing, regardless of the IP interface address or administrative state.
Examples

-> ip multicast spoofing static-source-ip 10.2.2.1
-> no ip multicast spoofing static-source-ip
-> ip multicast vlan 2 spoofing static-source-ip 10.2.2.1
-> no ip multicast vlan 2 spoofing static-source-ip
-> ip multicast vlan 3-5 spoofing static-source-ip 10.2.2.1
-> no ip multicast vlan 3-5 spoofing static-source-ip
-> ip multicast service 2 spoofing static-source-ip 11.2.2.1
-> no ip multicast service 2 spoofing static-source-ip
-> ip multicast service 3-5 spoofing static-source-ip 11.2.2.1
-> no ip multicast service 3-5 spoofing static-source-ip

Release History

Release 8.3.1.R02; command was added.
Release 8.4.1.R02; service parameter added.

Related Commands

show ip multicast Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigSpoofingStaticSourceAddress
**ip multicast zapping**

Enables or disables IGMP zapping on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```bash
ip multicast [vlan vlan_id[-vlan_id2] | service service_id] zapping [{enable | disable}]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zapping
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable`: Enable IGMP zapping.
- `disable`: Disable IGMP zapping.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the IGMP zapping is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- IGMP zapping refers to processing membership, immediate source filter removals and will not wait for the protocol's specified time period. This mode facilitates IP TV applications looking for quick changes between IP multicast groups.
- Use the **no** form of this command to restore the IGMP zapping status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

**Examples**

- `-> ip multicast zapping enable`
-> ip multicast zapping disable
-> no ip multicast zapping
-> ip multicast vlan 2 zapping enable
-> ip multicast vlan 3-5 zapping disable
-> no ip multicast vlan 2 zapping
-> no ip multicast vlan 3-5 zapping
-> ip multicast service 2 zapping enable
-> ip multicast service 3-5 zapping disable
-> no ip multicast service 2 zapping
-> no ip multicast service 3-5 zapping

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; service parameter added.

Related Commands

show ip multicast
Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigZapping
**ip multicast querier-forwarding**

Enables or disables IGMP querier forwarding on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querier-forwarding [enable | disable]

no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querier-forwarding
```

**Syntax Definitions**

- `vlan vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `enable`: Enable IGMP querier forwarding.
- `disable`: Disable IGMP querier forwarding.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the IGMP querier forwarding is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

- IGMP querier forwarding refers to promoting detected IGMP queriers to receive all IP multicast data traffic.

- Use the **no** form of this command to restore the IGMP querier forwarding status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

**Examples**

```
-> ip multicast querier-forwarding enable
```
-> ip multicast querier-forwarding disable
-> no ip multicast querier-forwarding
-> ip multicast vlan 2 querier-forwarding enable
-> no ip multicast vlan 3-5 querier-forwarding disable
-> ip multicast vlan 2 querier-forwarding
-> no ip multicast vlan 3-5 querier-forwarding
-> ip multicast service 2 querier-forwarding enable
-> ip multicast service 3-5 querier-forwarding
-> no ip multicast service 2 querier-forwarding
-> no ip multicast service 3-5 querier-forwarding

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; service parameter added.

**Related Commands**

`show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigQuerierForwarding
### ip multicast proxying

Enables or disables IGMP proxying on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying
```

#### Syntax Definitions

- `vlan_id[-vlan_id2]`  
  VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.

- `service_id[-service_id2]`  
  SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

- `enable`  
  Enable IGMP proxying.

- `disable`  
  Disable IGMP proxying.

#### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- If the IGMP proxying is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

- IGMP proxying refers to processing membership information on behalf of client systems and reporting membership on their behalf.

- Proxy reported IGMP packets are sent using the source MAC address of the proxying switch. Unless the spoofing feature is used, proxy reported IGMP packets will be sent using 0.0.0.0 for the IPv4 source address.

- Use the `no` form of this command to restore the IGMP proxying status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.
Examples

-> ip multicast proxying enable
-> ip multicast proxying disable
-> no ip multicast proxying
-> ip multicast vlan 2 proxying enable
-> ip multicast vlan 3-5 proxying disable
-> no ip multicast vlan 2 proxying
-> no ip multicast vlan 3-5 proxying
-> ip multicast service 2 proxying enable
-> ip multicast service 3-5 proxying disable
-> no ip multicast service 2 proxying
-> no ip multicast service 3-5 proxying

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; service parameter added.

Related Commands

show ip multicast

Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigProxying
**ip multicast helper-address**

Specifies the destination IP address of a relay host where IGMP host Reports and Leave messages are sent.

```
ip multicast [vlan vlan_id[-vlan_id2]] helper-address ip_address
```

```
no ip multicast [vlan vlan_id[-vlan_id2]] helper-address
```

### Syntax Definitions

- `vlan_id[-vlan_id2]`  	VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `ip_address`  
The IP address of the relay host.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip_address</code></td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- After the destination IP address is specified, the IPMS reporting feature is enabled.
- An operational IPv4 interface is required for the receiving LAN before any IGMP Reports and Leave messages can be relayed.
- Configuring a destination IP helper address is supported only in the VLAN domain; the service domain is not supported.
- Use the `no` form of this command to restore the IPMS reporting feature back to the default value (IP address 0.0.0.0) on the system. When the IP address is set to 0.0.0.0, the IPMS reporting feature is disabled.

### Examples

- `-> ip multicast helper-address 10.1.1.198`
- `-> no ip multicast helper-address`
- `-> ip multicast vlan 2 helper-address 10.1.1.198`
- `-> ip multicast vlan 3-5 helper-address 10.1.1.198`
- `-> no ip multicast vlan 2 helper-address`
-> no ip multicast vlan 3-5 helper-address

Release History
Release 7.1.1; command was introduced.
Release 8.4.1.R02; vlan parameter added.

Related Commands
show ip multicast Displays the IP Multicast Switching and Routing status and general configuration parameters,

MIB Objects
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigHelperAddress
**ip multicast zero-based-query**

Configures the use of an all-zero source IPv4 address for IGMP query packets when a non-querier is querying the membership of a port. This value is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable` Enable IGMP zero-based querying.
- `disable` Disable IGMP zero-based querying.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The IGMP zero-based query status set for a specific VLAN or SPB service overrides the zero-based query status set for the system.
- Use the **no** form of this command to restore the IGMP zero-based query status back to the default value (enabled) on the system, the specified VLAN, or the specified SPB service.

**Examples**

- `-> ip multicast zero-based-query enable`
- `-> ip multicast zero-based-query disable`
- `-> no ip multicast zero-based-query`
-> ip multicast vlan 2 zero-based-query enable
-> no ip multicast vlan 2 zero-based-query
-> no ip multicast vlan 3-5 zero-based-query
-> ip multicast vlan 3-5 zero-based-query enable
-> ip multicast service 10 zero-based-query disable
-> ip multicast service 10-15 zero-based-query disable
-> no ip multicast service 10 zero-based-query
-> no ip multicast service 10-15 zero-based-query disable

Release History

Release 8.3.1; command introduced.
Release 8.4.1; service parameter added.

Related Commands

show ip multicast  Displays the IP Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigZeroBasedQuery
**ip multicast forward-mode**

Configures the Layer 2 forwarding mode for IPv4 Multicast Switching (does not apply to IPv4 Multicast Routing). The forwarding mode is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```plaintext
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] forward-mode {asm | ssm | mac | auto}
```

```plaintext
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] forward-mode
```

### Syntax Definitions

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **service_id[-service_id2]**: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **asm**: Sets the IPMS forwarding mode to ASM (the bridge lookup is based on the packet group destination IP address). *This parameter is supported only in the VLAN domain; service domain is not supported.*
- **ssm**: Sets the IPMS forwarding mode to SSM (the bridge lookup is based on the packet source IP as well as the group destination IP). *This parameter is supported only in the VLAN domain; service domain is not supported.*
- **mac**: Sets the IPMS forwarding mode to MAC address (the bridge lookup is based on the MAC destination address).
- **auto**: Automatically determines the IPMS forwarding mode based on the current IGMP protocol version and the existing protocol state.

### Defaults

By default, the forwarding mode is set to automatic.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 32-51
Usage Guidelines

- The forwarding mode set for a specific VLAN or SPB service overrides the forwarding mode set for the system.

- If multicast routing is enabled on a VLAN, the following conditions apply:
  - On the OmniSwitch 9900, the bridging mode is independent of the routing mode. As a result, ASM bridging is allowed in a VLAN that has SSM routing configured or SSM bridging is allowed in a VLAN that has ASM routing configured.
  - Multicast routing is not supported on the OmniSwitch 6560 and OmniSwitch 6570M.
  - On all other OmniSwitch platforms, the routing configuration overrides the forwarding mode setting and determines the forwarding mode based on the group mappings. For example, BIDIR flows will use ASM while DVMRP flows and all other PIM modes will use SSM.

- Use the no form of this command to restore the Layer 2 forwarding mode back to the default value (automatic) on the system or the specified VLAN or SPB service.

Examples

- `-> ip multicast forward-mode auto`
- `-> ip multicast forward-mode asm`
- `-> ip multicast forward-mode ssm`
- `-> ip multicast forward-mode mac`
- `-> no ip multicast forward-mode`
- `-> ip multicast vlan 100 forward-mode auto`
- `-> ip multicast vlan 101-104 forward-mode asm`
- `-> ip multicast vlan 100 forward-mode ssm`
- `-> ip multicast vlan 101-104 forward-mode mac`
- `-> no ip multicast vlan 100 forward-mode`
- `-> no ip multicast vlan 101-104 forward-mode`
- `-> ip multicast service 10 forward-mode mac`
- `-> ip multicast service 11-15 forward-mode mac`
- `-> no ip multicast service 10 forward-mode`
- `-> no ip multicast service 11-15 forward-mode`

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; service parameter added.

Related Commands

```
show ip multicast
```
Displays the IP Multicast Switching and Routing status and general configuration parameters.

```
show ip multicast bridge
```
Displays the forwarding mode for IP multicast bridge table entries.

MIB Objects

```
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigForwardMode
```
**ip multicast update-delay-interval**

Sets the amount of time to delay IPv4 multicast forwarding updates on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval milliseconds
```

```
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval
```

### Syntax Definitions

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `milliseconds` The number of milliseconds to defer forwarding updates. Valid range is 0–10000.

### Defaults

By default, the forwarding update delay interval is set to zero.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When the forwarding update delay is set to zero, forwarding updates are processed immediately with minimal latency. Configuring a forwarding update delay value can limit the effects of persistent churn on the system.
- If the forwarding update delay interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Use the `no` form of this command to restore the forwarding update delay interval back to the default value (zero) on the system or the specified VLAN or SPB service.

### Examples

```
-> ip multicast update-delay-interval 10
-> no ip multicast update-delay-interval
```
-> ip multicast vlan 100 update-delay-interval 20
-> no ip multicast vlan 100 update-delay-interval
-> ip multicast service 20 update-delay-interval 20
-> no ip multicast service 20 update-delay-interval

**Release History**

Release 8.3.1; command was introduced.
Release 8.4.1.R02; service parameter added.

**Related Commands**

- `show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigUpdateDelayInterval`
**ip multicast fast-join**

Configures whether or not IP Multicast Switching will automatically create the forwarding entries in hardware as soon as the IGMP memberships are learned on the specified VLAN, Shortest Path Bridging (SPB) service or globally if no VLAN or SPB service is specified.

```plaintext
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] fast-join [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] fast-join
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs. *This parameter is supported only on the OmniSwitch 9900.*
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable`: Enable the IGMP fast join functionality.
- `disable`: Disable the IGMP fast join functionality.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command applies only to IPv4 Multicast Switching. If IP Multicast Routing is enabled, then the routing configuration will override the fast join setting.
- When the IP Multicast Switching fast join functionality is enabled, convergence of multicast traffic may occur faster because the forwarding entries are already created before the actual multicast traffic is received.
- When the IP Multicast Switching fast join functionality is disabled (the default), forwarding entries are not created in the hardware until the multicast traffic reaches the switch.
• If the IP Multicast Switching fast join is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

• Use the no form of this command to restore the IP Multicast Switching fast join setting back to the default value (disabled) on the system or the specified VLAN or SPB service.

**Examples**

-> ip multicast fast-join enable
-> ip multicast fast-join disable
-> no ip multicast fast-join
-> ip multicast service 10 fast-join enable
-> ip multicast service 11-15 fast-join disable
-> no ip multicast service 10 fast-join
-> no ip multicast service 11-15 fast-join

**Release History**

Release 8.3.1.R02; command introduced.
Release 8.4.1.R02; **vlan** and **service** parameters added.

**Related Commands**

**show ip multicast** Displays the IP Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigFastJoin
ip multicast host-list

Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

ip multicast host-list host_list_name ip_address [ip_address]
no ip multicast host-list host_list_name [ip_address]

Syntax Definitions

host_list_name  A name to assign to the host list (up to 20 characters).
ip_address  The IP address to add to the host list. Multiple IP addresses can be entered on the same command line.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

• Use the no form of this command to remove an IP address from the list or remove the entire list from the switch configuration.

• When the entire list is removed, any configuration associated with the list is also removed.

Examples

-> ip multicast host-list group-map1 10.1.1.198
-> ip multicast host-list ssm-map1 20.0.0.1
-> ip multicast host-list ssm-map2 30.0.0.1 30.0.0.2 30.0.0.3
-> no ip multicast host-list ssm-map2 30.0.0.2
-> no ip multicast host-list group-map1

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip multicast host-list  Displays the IP multicast host address list configuration for the switch.

MIB Objects

alaIpmsHostListTable
alaIpmsHostListName
alaIpmsHostListAddressType
alaIpmsHostListAddress
ip multicast ssm-map

Configures the translation of Any Source Multicast (ASM) group memberships into Source Specific Multicast (SSM) group memberships on the specified VLAN or on the system if no VLAN is specified.

```
ip multicast [vlan vlan_id] ssm-map {group_address/prefixLen host_list_name | admin-state {enable | disable}}
no ip multicast [vlan vlan_id] ssm-map group_address/prefixLen
```

**Syntax Definitions**

- **vlan_id**: VLAN on which to apply the mapping configuration.
- **group_address[/prefixLen]**: The multicast group address/prefix length to map to the host list. If no prefix length is specified, then the default length of 32 is used.
- **host_list_name**: The name of a host list to use for SSM mapping.
- **enable**: Enables the SSM mapping.
- **disable**: Disables the SSM mapping.

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- Use the **no** form of this command to remove the SSM mapping configuration from the system or the specified VLAN.
- If an SSM mapping is already enabled on the system, then the VLAN configuration will override the system's configuration.

**Examples**

- `-> ip multicast ssm-map 229.10.10.10 hostList1`
- `-> ip multicast ssm-map admin-state enable`
- `-> ip multicast vlan 200 ssm-map 225.11.11.11 hostList2`
- `-> ip multicast vlan 200 ssm-map admin-state enable`
- `-> no ip multicast ssm-map 229.10.10.10`

**Release History**

Release 8.3.1.R02; command was introduced.
**Related Commands**

- `show ip multicast ssm-map` Displays the SSM mapping configuration.
- `show ip multicast` Displays the IP Multicast Switching and Routing status and general configuration parameters, such as the SSM mapping setting.

**MIB Objects**

- `alaIpmsSsmMapTable`  
  - `alaIpmsSsmMapConfigType`
  - `alaIpmsSsmMapConfigAddressType`
  - `alaIpmsSsmMapConfigValue`
  - `alaIpmsSsmMapGroupAddress`
  - `alaIpmsSsmMapGroupPrefixLength`
  - `alaIpmsSsmMapSourceListName`
ip multicast initial-packet-buffer admin-state

Enables or disables initial packet buffering for IPv4 multicast flows on the specified VLAN or globally on the switch.

```
ip multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer admin-state {enable | disable}
```

**Syntax Definitions**

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **enable**: Enable the initial packet buffering globally on the switch.
- **disable**: Disable the initial packet buffering globally on the switch.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900V72/C32</th>
<th>6900</th>
<th>6900x48c6/t48c6/x48c4e/v48c8/c32e/t24c2/x24c2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When enabled, the following configuration is used for initial packet buffering on new multicast flows:
  - The maximum number of initial packets buffered per IPv4 multicast flow. Use the `ip multicast initial-packet-buffer max-packet` command to set this value.
  - The maximum number of IPv4 multicast flows that can be buffered. Use the `ip multicast initial-packet-buffer max-flow` command to set this value.
  - The maximum amount of time buffered packets are held if they are not sent out. Use the `ip multicast initial-packet-buffer timeout` command to set this value.
  - The minimum amount of time packets are held before delivery begins. Use the `ip multicast initial-packet-buffer min-delay` command to set this value.

- Configuring the status for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

**Examples**

- `-> ip multicast initial-packet-buffer admin-state disable`
- `-> ip multicast vlan 2 initial-packet-buffer admin-state enable`
- `-> ip multicast vlan 3-5 initial-packet-buffer admin-state enable`
**Release History**

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.

**Related Commands**

- **show ip multicast** Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

**MIB Objects**

alaIpmsConfigTable
- alaIpmsConfigType
- alaIpmsConfigAddressType
- alaIpmsConfigValue
- alaIpmsConfigInitialPacketBuffer
**ip multicast initial-packet-buffer max-packet**

Configures the maximum number of initial packets buffered per IPv4 multicast flow on the specified VLAN or globally on the switch.

```
ip multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer max-packet [num]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `num` The maximum number of packets allowed to buffer per IPv4 multicast flow. Valid range is 1–10.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>4</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

**Examples**

- `ip multicast initial-packet-buffer max-packet 4`
- `ip multicast vlan 2 initial-packet-buffer max-packet 10`
- `ip multicast vlan 3-5 initial-packet-buffer max-packet 10`

**Release History**

Release 8.2.1; command introduced.
Release 8.4.1.R02; `vlan` parameter added.
**Related Commands**

- `ip multicast initial-packet-buffer admin-state` Enables or disables the initial packet buffering feature globally on the switch for IPv4 multicast flows.
- `show ip multicast` Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

**MIB Objects**

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigInitialPacketBufferMaxPacket`
ip multicast initial-packet-buffer max-flow

Configures the maximum number of IPv4 multicast flows that can be buffered on the specified VLAN or globally on the switch.

```
ip multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer max-flow [num]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `num` The maximum number of IPv4 multicast flows allowed for initial packet buffering. Valid range is 1–32.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>32</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Required</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

**Examples**

- `-> ip multicast initial-packet-buffer max-flow 32`
- `-> ip multicast vlan 2 initial-packet-buffer max-flow 32`
- `-> ip multicast vlan 3-5 initial-packet-buffer max-flow 32`

**Release History**

- Release 8.2.1; command introduced.
- Release 8.4.1.R02; `vlan` parameter added.
Related Commands

- `ip multicast initial-packet-buffer admin-state` Enables or disables the initial packet buffering feature globally on the switch for IPv4 multicast flows.
- `show ip multicast` Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigInitialPacketBufferMaxFlow`
ip multicast initial-packet-buffer timeout

Configures the timeout value for the buffered IPv4 initial multicast packets on the specified VLAN or globally on the switch.

ip multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer timeout [seconds]

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id[-vlan_id2]</td>
<td>VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.</td>
</tr>
<tr>
<td>seconds</td>
<td>The timeout value for the initial buffered IPv4 multicast packets in seconds. Valid range is 1–10.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>10</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the buffered multicast packet is not sent out before the timeout, then the buffered packets will be removed from IPMS system.
- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

-> ip multicast initial-packet-buffer timeout 2
-> ip multicast vlan 2 initial-packet-buffer timeout 5
-> ip multicast vlan 3-5 initial-packet-buffer timeout t

Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; vlan parameter added.
### Related Commands

**ip multicast initial-packet-buffer admin-state**

Enables or disables the initial packet buffering feature globally on the switch, for IPv4 multicast flows.

**show ip multicast**

Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

### MIB Objects

alaIpmsConfigTable
- alaIpmsConfigType
- alaIpmsConfigAddressType
- alaIpmsConfigValue
- alaIpmsConfigInitialPacketBufferTimeout
**ip multicast initial-packet-buffer min-delay**

Configures the minimum delay to program the multicast replication index for IPv4 multicast flows buffered for initial packet on the specified VLAN or globally on the switch.

**ip multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer min-delay [milliseconds]**

---

**Syntax Definitions**

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **milliseconds**: The minimum delay value to program the multicast replication index for IPv4 multicast flows buffered for initial packet. Valid range is 0–1000.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliseconds</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

*Note.* This command configures a timer to delay the programming of multicast replication index in hardware which might increase the number of multicast packets lost during the learning phase.

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.

- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

**Examples**

- -> ip multicast initial-packet-buffer min-delay 200
- -> ip multicast vlan 2 initial-packet-buffer min-delay 200
- -> ip multicast vlan 3-5 initial-packet-buffer min-delay 200
**Release History**

Release 8.2.1; command introduced.
Release 8.4.1.R02; `vlan` parameter added.

**Related Commands**

- `ip multicast initial-packet-buffer admin-state`  
  Enables or disables the initial packet buffering feature globally on the switch for IPv4 multicast flows.

- `show ip multicast`  
  Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

**MIB Objects**

- `alaIpmsConfigTable`  
- `alaIpmsConfigType`  
- `alaIpmsConfigAddressType`  
- `alaIpmsConfigValue`  
- `alaIpmsConfigInitialPacketBufferMinDelay`
ip multicast display-interface-names

Sets the display output of the *show* commands listed below. When enabled, the display outputs for these commands will show the IP interface name for each VLAN associated with the IP multicast table entry.

```
ip multicast display-interface-names
no ip multicast display-interface-names
```

**Syntax Definitions**

N/A

**Defaults**

By default, this function is disabled. The display format is set to include the VLANs that are associated with the IP multicast source and forward flows.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to revert back to displaying the VLAN name.
- If there are any VLANs that are not configured with an IP interface or the IP interface is disabled, the output display will still include the VLAN when this function is enabled.
- This command may be helpful when reviewing output from multicast snooping commands and comparing state in multicast routing, which only interacts with IP interfaces.
- Enabling the display interface names option applies to the following *show* commands:
  
  ```
  show ip multicast forward
  show ip multicast neighbor
  show ip multicast querier
  show ip multicast group
  show ip multicast source
  show ip multicast tunnel
  ```

- The command examples provided display the *show ip multicast source* output after the display interface name function is turned on (enabled) and off (disabled).
Examples

-> ip multicast display-interface-name  
-> show ip multicast source

Total 11 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>239.192.1.17</td>
<td>172.1.1.1</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.18</td>
<td>172.1.1.2</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.19</td>
<td>172.1.1.3</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.20</td>
<td>172.1.1.4</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.21</td>
<td>172.1.1.5</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.22</td>
<td>172.1.1.6</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.23</td>
<td>172.1.1.7</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.24</td>
<td>172.1.1.8</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.25</td>
<td>172.1.1.9</td>
<td>0.0.0.0</td>
<td>VL-10</td>
</tr>
<tr>
<td>239.192.1.9</td>
<td>173.1.1.9</td>
<td>0.0.0.0</td>
<td>VL-20</td>
</tr>
<tr>
<td>239.192.1.10</td>
<td>173.1.1.10</td>
<td>0.0.0.0</td>
<td>VL-20</td>
</tr>
</tbody>
</table>

-> no ip multicast display-interface-name  
-> show ip multicast source

Total 11 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>239.192.1.17</td>
<td>172.1.1.1</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.18</td>
<td>172.1.1.2</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.19</td>
<td>172.1.1.3</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.20</td>
<td>172.1.1.4</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.21</td>
<td>172.1.1.5</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.22</td>
<td>172.1.1.6</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.23</td>
<td>172.1.1.7</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.24</td>
<td>172.1.1.8</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.25</td>
<td>172.1.1.9</td>
<td>0.0.0.0</td>
<td>vlan 1001</td>
</tr>
<tr>
<td>239.192.1.9</td>
<td>173.1.1.9</td>
<td>0.0.0.0</td>
<td>vlan 2001</td>
</tr>
<tr>
<td>239.192.1.10</td>
<td>173.1.1.10</td>
<td>0.0.0.0</td>
<td>vlan 2001</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1.R02; command was introduced.
**Related Commands**

- `show ip multicast source`  
  Displays the IP Multicast Switching and Routing source table entries.
- `show ip multicast forward`  
  Displays the IP Multicast Switching and Routing forwarding table entries.

**MIB Objects**

alaIpmsGlobalConfigTable
  - `alaIpmsGlobalConfigAddressType`
  - `alaIpmsGlobalConfigDisplayInterfaceNames`
**ip multicast inherit-default-vrf-config**

Configures whether or not the global IPMS configuration defined in the default VRF instance is applied to all VRF instances.

**ip multicast inherit-default-vrf-config**

**no ip multicast inherit-default-vrf-config**

---

**Syntax Definitions**

N/A

**Defaults**

By default, the global IPMS configuration defined in the default VRF instance is applied to all VRF instances on the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable this function. When disabled, the global IPMS configuration defined in the default VRF instance is not applied to all other VRF instances on the switch.

- When enabled (the default), additional VRF instances will inherit the global IPMS configuration defined in the default VRF instance.

- A global IPMS configuration defined for a specific non-default VRF instance takes precedence over the global IPMS configuration defined for the default VRF.

- Note that any per-VLAN IPMS configuration defined in a non-default VRF instance will show up as part of the default VRF instance in the configuration snapshot file. However, the functionality is still applied within the context of VRF instance in which the per-VLAN configuration was originally defined.

**Examples**

- `-> ip multicast inherit-default-vrf-config`
- `-> no ip multicast inherit-default-vrf-config`
Release History
Release 8.3.1; command introduced.

Related Commands

show ip multicast
Displays the status and configuration parameters of initial multicast packet buffer for IPv4 flows on the system.

MIB Objects
alaIpmsGlobalConfigTable
   alaIpmsGlobalConfigAddressType
   alaIpmsGlobalConfigInheritDefaultVrfConfig
ip multicast profile

Defines an IPMS profile that is used to apply a pre-defined configuration to the global IPMS instance (all VLAN and service instances) or to a specific VLAN or service instance. Using a configuration profile to configure IPMS functionality avoids having to configure each IPMS parameter with a separate CLI command.

This section describes the base command (ip multicast profile) along with optional command keywords that are used to configure IPMS parameter values that are applied when the profile is assigned to an IPMS instance. Optional keywords are listed separately but can be entered in combination on the same command line. Use the no form for the keywords to change a specific parameter value for the profile.

There is a “default” profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance. The default profile cannot be deleted, but the profile parameter values are configurable through this command.

ip multicast profile profile_name
    [admin-state {enable | disable}]
    [flood-unknown {enable | disable}]
    [version version]
    [robustness robustness]
    [querying {enable | disable}]
    [query-interval [seconds]]
    [query-response-interval [tenths-of-seconds]]
    [last-member-query-interval [tenths-of-seconds]]
    [unsolicited-report-interval [seconds]]
    [proxying {enable | disable}]
    [spoofing {enable | disable}]
    [spoofing static-source-ip ip_address]
    [zapping {enable | disable}]
    [querier-forwarding {enable | disable}]
    [router-timeout [seconds]]
    [source-timeout [seconds]]
    [max-group [num] [action {none | drop | replace}]]
    [helper-address [ip_address]]
    [zero-based-query {enable | disable}]
    [forward-mode {asm | ssm | mac | auto}]
    [update-delay-interval milliseconds]
    [fast-join {enable | disable}]
    [initial-packet-buffer admin-state {enable | disable}]
    [initial-packet-buffer max-flow [num]]
    [initial-packet-buffer max-packet [num]]
    [initial-packet-buffer timeout [seconds]]
    [initial-packet-buffer min-delay [milliseconds]]

no ip multicast profile profile_name [admin-state | flood-unknown | version | robustness | ...]
**Syntax Definitions**

`profile_name` The name to associate with the IPMS profile.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an IPMS profile from the switch configuration.
- To change the value of a specific profile parameter, specify the parameter keyword with this command. For example, `no ip multicast profile ipms-1 admin-state`, `ip multicast profile ipms-1 query-interval 100`, or `ip multicast profile ipms-1 querying enable`. The new parameter values are applied to all IPMS instances to which the profile is assigned.
- The profile name must already exist in the switch configuration before parameter values can be modified. Use this command to create the profile first, then configure the profile parameter values.
- For more information about specific profile parameter values, refer to the following explicit IPMS configuration commands for each profile parameter:

<table>
<thead>
<tr>
<th>Port Template Parameter</th>
<th>Explicit Port Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>[admin-state {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[flood-unknown {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[version version]</td>
<td>ip multicast version</td>
</tr>
<tr>
<td>[robustness robustness]</td>
<td>ip multicast robustness</td>
</tr>
<tr>
<td>[querying {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[query-interval [seconds]]</td>
<td>ip multicast query-interval</td>
</tr>
<tr>
<td>[query-response-interval [tenths-of-seconds]]</td>
<td>ip multicast query-response-interval</td>
</tr>
<tr>
<td>[last-member-query-interval [tenths-of-seconds]]</td>
<td>ip multicast last-member-query-interval</td>
</tr>
<tr>
<td>[unsolicited-report-interval [seconds]]</td>
<td>ip multicast unsolicited-report-interval</td>
</tr>
<tr>
<td>[proxying {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[spoofing {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[spoofing static-source-ip ip_address]</td>
<td>ip multicast spoofing static-source-ip</td>
</tr>
</tbody>
</table>
IP Multicast Switching Commands

<table>
<thead>
<tr>
<th>Port Template Parameter</th>
<th>Explicit Port Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>[zapping {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[querier-forwarding {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[router-timeout [seconds]]</td>
<td>ip multicast router-timeout</td>
</tr>
<tr>
<td>[source-timeout [seconds]]</td>
<td>ip multicast source-timeout</td>
</tr>
<tr>
<td>[max-group [num] [action {none</td>
<td>drop</td>
</tr>
<tr>
<td>[helper-address [ip_address]]</td>
<td>ip multicast helper-address</td>
</tr>
<tr>
<td>[zero-based-query {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[forward-mode {asm</td>
<td>ssm</td>
</tr>
<tr>
<td>[update-delay-interval milliseconds]</td>
<td>ip multicast update-delay-interval</td>
</tr>
<tr>
<td>[fast-join {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[initial-packet-buffer admin-state {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[initial-packet-buffer max-flow [num]]</td>
<td>ip multicast initial-packet-buffer max-flow</td>
</tr>
<tr>
<td>[initial-packet-buffer max-packet [num]]</td>
<td>ip multicast initial-packet-buffer max-packet</td>
</tr>
<tr>
<td>[initial-packet-buffer timeout [seconds]]</td>
<td>ip multicast initial-packet-buffer timeout</td>
</tr>
<tr>
<td>[initial-packet-buffer min-delay [milliseconds]]</td>
<td>ip multicast initial-packet-buffer min-delay</td>
</tr>
</tbody>
</table>

**Examples**

- `-> ip multicast profile “IGMPv3 with Zapping”`
- `-> ip multicast profile “IGMPv3 with Zapping” admin-state enable`
- `-> ip multicast profile “IGMPv3 with Zapping” zapping enable version 3`
- `-> ip multicast profile “IGMPv3 with Zapping” fast-join enable proxying enable`
- `-> no ip multicast profile “IGMPv3 with Zapping” proxying`
- `-> no ip multicast profile “IGMPv3 with Zapping”`

**Release History**

Release 8.4.1.R02; command was introduced.

**Related Commands**

**ip multicast apply-profile**

Assigns an IPMS configuration profile globally for the switch or to a specific VLAN or service instance.

**show ip multicast**

Displays the profile assignment for the IPMS instance.

**show ip multicast profile**

Displays the IPMS profile configuration.
MIB Objects

alaIpmsProfileTable
  alaIpmsProfileAddressType
  alaIpmsProfileName
  alaIpmsProfileIndex
  alaIpmsProfileRowStatus
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigProfileName
**ip multicast apply-profile**

Assigns the name of an existing IPMS configuration profile to the global IPMS instance (all VLANs and services) or to a specific VLAN or Shortest Path Bridging (SPB) service instance. An IPMS configuration profile defines parameter options that are applied to the IPMS instance to which the profile is assigned.

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] apply-profile profile_name
```

```
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] apply-profile
```

### Syntax Definitions

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **service_id[-service_id2]**: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **profile_name**: The name to associate with the IPMS profile.

### Defaults

There is a “default” profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to revert the profile assignment back to the “default” profile.
- Specify a range of VLANs (**vlan 20-25**) or a range of SPB services (**service 10-15**) to apply the specified profile to multiple VLANs or services with one CLI command.
- The specified profile name must already exist in the switch configuration.

### Examples

- `-> ip multicast apply-profile “IGMPv3 with Zapping”`
- `-> ip multicast vlan 20 apply-profile “IGMPv3 with Zapping”`
- `-> ip multicast vlan 20-25 apply-profile “IGMPv3 with Zapping”`
- `-> ip multicast service 10 apply-profile “IGMPv3 with Zapping”`
- `-> ip multicast service 10-15 apply-profile “IGMPv3 with Zapping”`
- `-> no ip multicast apply-profile`
-> no ip multicast vlan 20 apply-profile
-> no ip multicast vlan 20-15 apply-profile
-> no ip multicast service 10 apply-profile
-> no ip multicast service 10-15 apply-profile

**Release History**

Release 8.4.1.R02; command was introduced.

**Related Commands**

- **ip multicast profile**
  Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.

- **show ip multicast**
  Displays the profile assignment for the IPMS instance.

- **show ip multicast profile**
  Displays the IPMS profile configuration.

**MIB Objects**

- **alaIpmsProfileTable**
  laIpmsProfileAddressType
  laIpmsProfileName
  laIpmsProfileIndex
  laIpmsProfileRowStatus

- **alaIpmsConfigTable**
  laIpmsConfigType
  laIpmsConfigAddressType
  laIpmsConfigValue
  laIpmsConfigProfileName
**ipv6 multicast admin-state**

Enables or disables IPv6 Multicast Switching and Routing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id1[-vlan_id2] | service service_id1[-service_id2]] admin-state [enable | disable]

no ipv6 multicast [vlan vlan_id1[-vlan_id2] | service service_id1[-service_id2]] admin-state
```

### Syntax Definitions

- **vlan_id1[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **service_id1[-service_id2]**: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- **enable**: Enable IPv6 Multicast Switching and Routing.
- **disable**: Disable IPv6 Multicast Switching and Routing.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The configuration of an IPv6 multicast routing protocol on an IPv6 interface operationally triggers IP Multicast Switching and Routing functionality on any underlying VLAN or SPB service. This occurs regardless of any explicit IPMS configuration, such as attempting to specifically disable IPMS.
- If there is no IPv6 Multicast routing protocol already running on the switch, then the `ipv6 multicast admin-state` command alone controls IPMS operations.
- Enabling IPMS on individual VLANs or services, as needed, is recommended to conserve switch resources.
• If the IPv6 Multicast Switching and Routing is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

**Note.** Globally enabling the IPv6 Multicast Switching and Routing status for the switch only applies to the VLAN domain (does not apply to the service domain). As a result, IPv6 Multicast Switching and Routing must be explicitly enabled or disabled for each SPB service. However, globally disabling IPMS for all SPB services is supported.

• Use the `no` form of this command to restore the IPv6 Multicast Switching and Routing status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

**Examples**

```
-> ipv6 multicast admin-state enable
-> ipv6 multicast admin-state disable
-> no ipv6 multicast admin-state
-> ipv6 multicast vlan 2 admin-state enable
-> ipv6 multicast vlan 3-5 admin-state disable
-> no ipv6 multicast vlan 2 admin-state
-> no ipv6 multicast vlan 3-5 admin-state
-> ipv6 multicast service 10 admin-state enable
-> ipv6 multicast service 11-15 admin-state disable
-> no ipv6 multicast service 10 admin-state
-> no ipv6 multicast service 11-15 admin-state
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

`show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

```
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigStatus
```
**ipv6 multicast flood-unknown**

Enables or disables the flooding of initial unknown multicast traffic for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified. When a traffic flow is first seen on a port, there is a brief period of time where traffic may get dropped before the forwarding information is calculated. When flooding unknown multicast traffic is enabled, no packets are dropped before the forwarding information is available.

```bash
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] flood-unknown [enable | disable]
```

```bash
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] flood-unknown
```

### Syntax Definitions

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `enable`: Enable flooding of unknown traffic until it is learned.
- `disable`: Disable flooding of unknown traffic.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If this command function is enabled after the system is up and running, the flooding of unknown multicast traffic only applies to new flows.
- On an OmniSwitch 6860, OmniSwitch 6865, and OmniSwitch 6900:
  - Configuring the flood unknown status for any VLAN enforces the flood unknown behavior globally across all VLANs. The IPv4 multicast version of this command (`ip multicast flood-unknown`), however, enforces the flood unknown behavior at the per-VLAN level.
  - IPv6 multicast snooping for VLANs does not snoop ff02::/64 and the traffic is allowed to flood...
even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded IPv6 addresses.

- When IPv6 multicast snooping is enabled for any service, the flooding of unknown multicast traffic is unconditionally enforced for all snooping services; this is the only supported flood unknown behavior for services.

- IPv6 multicast snooping for services does not snoop MAC addresses that fall within the range of 01:00:5e:00:00:00/40 and 33:33:00:00:00:00/40 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to the excluded MAC addresses.

- On an OmniSwitch 9900, IPv6 multicast snooping for VLANs or services does not snoop ff02::/120 and the traffic is allowed to flood even if the flooding of unknown multicast traffic is disabled. Avoid using any multicast groups that map to these excluded IPv6 addresses.

- Use this command to provide an "open failure" strategy for when hardware resource conflicts or software limits prevent the traffic from being registered in the fast path.

- Use the no form of this command to restore the flooding of unknown traffic back to the default value (disabled) on the system.

Examples

-> ipv6 multicast flood-unknown enable
-> ipv6 multicast flood-unknown disable
-> no ipv6 multicast flood-unknown
-> ipv6 multicast vlan 100 flood-unknown enable
-> ipv6 multicast vlan 101-105 flood-unknown enable
-> ipv6 multicast vlan 100 flood-unknown disable
-> no ipv6 multicast vlan 100 flood-unknown
-> no ipv6 multicast vlan 101-105 flood-unknown
-> ipv6 multicast service 10 flood-unknown enable
-> ipv6 multicast service 11-15 flood-unknown enable
-> ipv6 multicast service 10 flood-unknown disable
-> no ipv6 multicast service 10 flood-unknown
-> no ipv6 multicast service 11-15 flood-unknown

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; vlan and service parameter added.

Related Commands

- show ipv6 multicast Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigFloodUnknown
**ipv6 multicast version**

Sets the default version of the MLD protocol on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] version [version]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] version
```

**Syntax Definitions**

- `vlan vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `version` Default MLD protocol version to run. Valid entries are 1 or 2.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IPv6 Multicast Switching and Routing must be enabled to set the default MLD protocol version on the system and/or the specified VLANs. or SPB services.
- If the default MLD protocol version is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Due to protocol inter-operation requirements, this command specifies only a default version of the MLD protocol to run.
- Use the `no` form of this command to restore the MLD multicast version back to the default value (version 1) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, ipv6 multicast version 0).
**Examples**

- `ipv6 multicast version 2`
- `ipv6 multicast version 0`
- `no ipv6 multicast version`
- `ipv6 multicast vlan 2 version 2`
- `ipv6 multicast vlan 3-5 version 2`
- `ipv6 multicast vlan 2 version 0`
- `no ipv6 multicast vlan 2 version`
- `ipv6 multicast vlan 3-5 version`
- `ipv6 multicast service 2 version 3`
- `ipv6 multicast service 3-5 version 3`
- `ipv6 multicast service 2 version 0`
- `no ipv6 multicast service 2 version`
- `no ipv6 multicast service 3-5 version`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

`show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

`alaIpmsConfigTable`
  `alaIpmsConfigType`
  `alaIpmsConfigAddressType`
  `alaIpmsConfigValue`
  `alaIpmsConfigVersion`
**ipv6 multicast port max-group**

Configures the maximum group limit learned per port. The limit is applicable on the given port for all VLAN instances or all SPB service instances of the port.

```
ipv6 multicast {port chassis/slot/port | sap port sap_id} max-group [num] [action {none | drop | replace}]
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port</td>
<td>The slot and port number (3/1).</td>
</tr>
<tr>
<td>sap_id</td>
<td>The SAP ID (chassis/slot/port:encapsulation). <em>This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.</em></td>
</tr>
<tr>
<td>num</td>
<td>The maximum MLD group count. Valid range is 0–4294967295.</td>
</tr>
<tr>
<td>none</td>
<td>Disables the maximum group limit configuration.</td>
</tr>
<tr>
<td>drop</td>
<td>Drops the incoming membership request.</td>
</tr>
<tr>
<td>replace</td>
<td>Replaces an existing membership with the incoming membership request. A leave is not sent to the router for the replaced group.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, the max-group limit is set to zero.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If group memberships are already registered on a port/VLAN or SAP port/SPB service instance and the group limit is set to a lower value for the instance, the current group memberships are not removed until they expire. The effect of the new lower group limit value is applied when one of the following occurs to help avoid any undetermined behavior:
  - IP multicast memberships are aged out on a port/VLAN or SAP port/SPB service instance.
  - IP multicast memberships are pruned by a leave or when IP multicast is disabled on the specific VLAN or SPB service or globally disabled for the switch.
The configuration is allowed even when the IP multicast status is disabled.

If the `num` and `action` parameters are not specified, then the limit is removed.

When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ip multicast sap port 1/1/23:10 max-group 10 action drop`, where `1/1/23:10` is the SAP ID).

A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port `1/1/23` with VLAN 10 encapsulation is `1/1/23:10`. Any traffic received on port `1/1/23` that is tagged with VLAN 10 is mapped to the SPB service that is associated with the `1/1/23:10` SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

The maximum group configuration on a port will override the VLAN, SPB service, or global configuration.

MLD zapping must be enabled when the maximum group limit is enabled and the action is dropped.

The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
- Group limit configured for a port or an SPB SAP port.
- Group limit configured for a specific VLAN or SPB service.
- Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
- Group limit configured for a VLAN or SPB service within a specific VRF context.
- Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.

**Examples**

```bash
-> ipv6 multicast port 1/1/12 max-group 10 action drop
-> ipv6 multicast port 1/1/14 max-group action replace
-> ipv6 multicast port 1/1/14 max-group
-> ipv6 multicast sap port 1/1/23:10 max-group 10 action drop
-> ipv6 multicast sap port 1/1/26:20.200 max-group 20 action replace
-> ipv6 multicast sap port 1/1/16:20.200 max-group
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `sap port` parameter added.

**Related Commands**

- `show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.
- `show ipv6 multicast port` Displays the maximum group configuration for VLAN ports or SPB service SAP ports.

**MIB Objects**

- `alaIpmsIntfTable`  
- `alaIpmsIntfConfigType`  
- `alaIpmsIntfAddressType`  
- `alaIpmsIntfMaxGroupLimit`
alaIpmsIntfMaxGroupExceedAction
**ipv6 multicast max-group**

Configures the maximum group limit learned per port for the specified VLAN, Shortest Path Bridging (SPB) service, or per port on the system if no VLAN or SPB service is specified. The limit is applied to each port that is a member of the given VLAN or SPB service and the specified action is taken when the limit is exceeded.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] max-group [num] [action {none | drop | replace}]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `num` The maximum MLD group count. Valid range is 0–4294967295.
- `none` Disables the maximum group limit configuration.
- `drop` Drops the incoming membership request.
- `replace` Replaces an existing membership with the incoming membership request.

**Defaults**

By default, the max-group limit is set to zero.

<table>
<thead>
<tr>
<th>parameter</th>
<th>defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>none</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a VLAN or SPB service is not specified, this command configures the global maximum group limit applied to all VLAN ports and SPB Service Access Point (SAP) ports.
- If a VLAN is specified, this command configures the maximum group limit learned per port on a VLAN. The limit is applied to each port that is a member of the given VLAN.
If an SPB service is specified, this command configures the maximum group limit learned per port on an SPB service. The limit is applied to each port that is a member of the given SPB service.

Configuring a maximum group value will have no affect on existing group memberships until the memberships are refreshed on the port/VLAN or port/SPB service instance.

The configuration of a maximum group limit is allowed even when the IP multicast status is disabled.

If the `num` and `action` parameters are not specified, then the limit is removed.

The maximum group configuration on a VLAN or SPB service will override the global configuration.

The maximum group configuration is applied in the following order of precedence (listed from highest to lowest precedence):
- Group limit configured for a port or an SPB SAP port.
- Group limit configured for a specific VLAN or SPB service.
- Group limit configured for the IPMS profile assigned to a VLAN or SPB service.
- Group limit configured for a VLAN or SPB service within a specific VRF context.
- Group limit configured for the IPMS profile assigned to a VLAN or SPB service within a specific VRF context.

MLD zapping must be enabled when the max-group limit is enabled and the action is dropped.

**Examples**

```
-> ipv6 multicast max-group 10 action drop
-> ipv6 multicast max-group 20 action replace
-> ipv6 multicast max-group
-> ipv6 multicast vlan 10 max-group 10 action drop
-> ipv6 multicast vlan 20 max-group action drop
-> ipv6 multicast vlan 11-15 max-group 10 action replace
-> ipv6 multicast service 5 max-group 10 action drop
-> ipv6 multicast service 20 max-group action drop
-> ipv6 multicast service 10-15 max-group 10 action replace
-> ipv6 multicast service 5 max-group
-> ipv6 multicast service 10-15 max-group
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

`show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`
- `alaIpmsConfigType`
- `alaIpmsConfigAddressType`
- `alaIpmsConfigValue`
- `alaIpmsConfigMaxGroupLimit`
alaIpmsConfigMaxGroupExceedAction
ipv6 multicast static-neighbor

Creates a static MLD neighbor entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

ipv6 multicast static-neighbor vlan vlan_id {port chassis/slot/port | linkagg agg_id}
ipv6 multicast static-neighbor service service_id sap {port | linkagg} {sap_id}

no ipv6 multicast static-neighbor vlan vlan_id {port chassis/slot/port | linkagg agg_id}
no ipv6 multicast static-neighbor service service_id sap {port | linkagg} {sap_id}

---

Syntax Definitions

- **vlan_id**: VLAN to include as a static MLD neighbor.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number to configure as a static MLD neighbor.
- **agg_id**: The link aggregate to configure as a static MLD neighbor.
- **service_id**: SPB service ID to include as a static MLD neighbor. The valid range is 1–32767. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- **sap_id**: The SAP ID (chassis/slot/port:encapsulation). This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.

---

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to remove an MLD static neighbor entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an MLD static neighbor entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the MLD traffic and IPv6 multicast traffic.
- To create an MLD static neighbor entry on a link aggregate, use the **linkagg** parameter (for example, ipv6 multicast static-neighbor vlan 2 linkagg 7 or ipv6 multicast static-neighbor service 10 sap linkagg 10:100).
• When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ipv6 multicast static-neighbor service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).

• A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

**Examples**

```
-> ipv6 multicast static-neighbor vlan 4 port 1/1
-> no ipv6 multicast static-neighbor vlan 4 port 1/1
-> ipv6 multicast static-neighbor vlan 4 port 7
-> no ipv6 multicast static-neighbor vlan 4 port 7

-> ipv6 multicast static-neighbor service 10 sap port 1/1/2:100
-> no ipv6 multicast static-neighbor service 10 sap port 1/1/2:100
-> ipv6 multicast static-neighbor service 10 sap linkagg 10:100
-> no ipv6 multicast static-neighbor service 10 sap linkagg 10:100
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.1; `linkagg` parameter was added.
Release 8.4.1; `service` and `sap` parameters added.

**Related Commands**

`show ipv6 multicast neighbor` Displays the MLD neighbor table entries of IPv6 Multicast Switching and Routing.

**MIB Objects**

- `alaIpmsStaticNeighborTable`
- `alaIpmsStaticNeighborConfigType`
- `alaIpmsStaticNeighborAddressType`
- `alaIpmsStaticNeighborValue`
- `alaIpmsStaticNeighborIfIndex`
- `alaIpmsStaticNeighborSubValue`
- `alaIpmsStaticNeighborRowStatus`
**ipv6 multicast static-querier**

Creates a static MLD querier entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

```
ipv6 multicast static-querier vlan vlan_id {port chassis/slot/port | linkagg agg_id}
ipv6 multicast static-querier service service_id sap {port | linkagg} {sap_id}
```

```
no ipv6 multicast static-querier vlan vlan_id {port chassis/slot/port | linkagg agg_id}
no ipv6 multicast static-querier service service_id sap {port | linkagg} {sap_id}
```

**Syntax Definitions**

- `vlan_id`: VLAN to include as a static MLD querier.
- `chassis`: The chassis identifier.
- `slot/port`: The slot and port number to configure as a static MLD querier.
- `agg_id`: The link aggregate to configure as a static MLD querier.
- `service_id`: SPB service ID to include as a static MLD querier. The valid range is 1–32767. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `sap_id`: The SAP ID (chassis/slot/port:encapsulation). This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an MLD static querier entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.
- Creating an MLD static querier entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive all of the MLD traffic.
- To create an MLD static querier entry on a link aggregate, use the `linkagg` parameter (for example, `ipv6 multicast static-querier vlan 2 linkagg 7` or `ipv6 multicast static-querier service 10 sap linkagg 10:100`).
• When using the sap port parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, ipv6 multicast static-neighbor service 10 sap port 1/1/23:10, where 1/1/23:10 is the SAP ID).

• A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

Examples

-> ipv6 multicast static-querier vlan 4 port 1/1
-> no ipv6 multicast static-querier vlan 4 port 1/1
-> ipv6 multicast static-querier vlan 4 port 7
-> no ipv6 multicast static-querier vlan 4 port 7

-> ipv6 multicast static-querier service 10 sap port 1/1/2:100
-> no ipv6 multicast static-querier service 10 sap port 1/1/2:100
-> ipv6 multicast static-querier service 10 sap linkagg 10:100
-> no ipv6 multicast static-querier service 10 sap linkagg 10:100

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; linkagg parameter was added.
Release 8.4.1; service and sap parameters added.

Related Commands

show ipv6 multicast querier Displays the MLD querier table entries of IPv6 Multicast Switching and Routing.

MIB Objects

alaIpmnStaticQuerierTable
alaIpmnStaticQuerierConfigType
alaIpmnStaticQuerierAddressType
alaIpmnStaticQuerierValue
alaIpmnStaticQuerierIfIndex
alaIpmnStaticQuerierSubValue
alaIpmnStaticQuerierRowStatus
**ipv6 multicast static-group**

Creates a static MLD group entry on the specified port for the specified VLAN or on the specified Service Access Point (SAP) port for the specified Shortest Path Bridging (SPB) service.

```plaintext
ipv6 multicast static-group ipv6_address vlan vlan_id {port chassis/slot/port | linkagg agg_id}
ipv6 multicast static-group ipv6_address service service_id sap {port | linkagg} {sap_id}
no ipv6 multicast static-group ipv6_address vlan vlan_id {port chassis/slot/port | linkagg agg_id}
no ipv6 multicast static-group ipv6_address service service_id sap {port | linkagg} {sap_id}
```

**Syntax Definitions**

- `ipv6_address`: IPv6 multicast group address.
- `vlan_id`: VLAN to include as a static MLD group.
- `chassis`: The chassis identifier.
- `slot/port`: The slot and port number to configure as a static MLD group.
- `agg_id`: The link aggregate to configure as a static MLD group.
- `service_id`: SPB service ID to include as a static MLD group. The valid range is 1–32767. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `sap_id`: The SAP ID (chassis/slot/port:encapsulation). *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an MLD static group entry on the specified port for the specified VLAN or on the specified SAP port for the specified SPB service.

- Creating an MLD static group entry on the specified port/VLAN or the specified SAP port/service, enables that network segment to receive MLD traffic addressed to the specified IP multicast group address.
To create an MLD static group entry on a link aggregate, use the `linkagg` parameter (for example, `ipv6 multicast static-group 225.0.0.1 vlan 2 linkagg 7` or `ipv6 multicast static-group 225.0.0.1 service 10 sap linkagg 10:100`).

When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ipv6 multicast static-querier service 10 sap port 1/1/23:10`, where `1/1/23:10` is the SAP ID).

A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port `1/1/23` with VLAN `10` encapsulation is `1/1/23:10`. Any traffic received on port `1/1/23` that is tagged with VLAN `10` is mapped to the SPB service that is associated with the `1/1/23:10` SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.

**Examples**

```
-> ipv6 multicast static-group ff05::4681 vlan 4 port 1/1
-> no ipv6 multicast static-group ff05::4681 vlan 4 port 1/1
-> ipv6 multicast static-group ff05::4681 vlan 4 port 7
-> no ipv6 multicast static-group ff05::4681 vlan 4 port 7

-> ipv6 multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100
-> no ipv6 multicast static-group 229.10.10.10 service 10 sap port 1/1/2:100
-> ipv6 multicast static-group 225.11.11.11 service 10 sap linkagg 10:100
-> no ipv6 multicast static-group 225.11.11.11 service 10 sap linkagg 10:100
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.1; `linkagg` parameter was added.
Release 8.4.1; `service` and `sap` parameters added.

**Related Commands**

- `show ipv6 multicast group` Displays the MLD group membership table entries of IPv6 Multicast Switching and Routing for the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

**MIB Objects**

```
alaIpmsStaticMemberTable
   alaIpmsStaticMemberConfigType
   alaIpmsStaticMemberAddressType
   alaIpmsStaticMemberValue
   alaIpmsStaticMemberIfIndex
   alaIpmsStaticMemberSubValue
   alaIpmsStaticMemberGroupAddress
   alaIpmsStaticMemberRowStatus
```
**ipv6 multicast query-interval**

Sets the MLD query interval on the specified VLAN, Shortest Path Bridging (SPB), or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id|-vlan_id2] | service service_id|-service_id2] query-interval [seconds]
no ipv6 multicast [vlan vlan_id|-vlan_id2] | service service_id|-service_id2] query-interval
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `seconds` MLD query interval in seconds. Valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>125</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IPv6 Multicast Switching and Routing must be enabled to set the MLD query interval on the system and/or the specified VLANs or SPB services.
- If the MLD query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The MLD query interval refers to the time period between MLD query messages.
- Due to protocol inter-operation requirements, this command specifies only a default version of the MLD query interval to use.
- Use the **no** form of this command to restore the MLD query interval back to the default value (125 seconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a
value of 0 with this command also restores the default value (for example, `ipv6 multicast query-interval 0`).

**Examples**

- `ipv6 multicast query-interval 100`
- `ipv6 multicast query-interval 0`
- `no ipv6 multicast query-interval`
- `ipv6 multicast vlan 2 query-interval 100`
- `ipv6 multicast vlan 3-5 query-interval 100`
- `ipv6 multicast vlan 2 query-interval 0`
- `no ipv6 multicast vlan 2 query-interval`
- `no ipv6 multicast vlan 3-5 query-interval`
- `ipv6 multicast service 2 query-interval 100`
- `ipv6 multicast service 3-5 query-interval 100`
- `ipv6 multicast service 2 query-interval 0`
- `no ipv6 multicast service 2 query-interval`
- `no ipv6 multicast service 3-5 query-interval`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

**show ipv6 multicast** Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable

alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigQueryInterval
**ipv6 multicast last-member-query-interval**

Sets the MLD last member query interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] last-member-query-interval [milliseconds]
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] last-member-query-interval
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `milliseconds` MLD last member query interval in milliseconds. Valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>milliseconds</code></td>
<td>1000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IPv6 Multicast Switching and Routing must be enabled to set the MLD last member query interval to use on the system and/or the specified VLANs or SPB services.
- If the MLD last member query interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The MLD last member query interval refers to the time period to reply to an MLD query message sent in response to a leave group message.
- Use the `no` form of this command to restore the MLD last member query interval back to the default value (1000 milliseconds) on the system, the specified VLAN, or the specified SPB service.
addition, specifying a value of 0 with this command also restores the default value (for example, `ipv6 multicast last-member-query-interval 0`).

**Examples**

```
-> ipv6 multicast last-member-query-interval 2200
-> ipv6 multicast last-member-query-interval 0
-> no ipv6 multicast last-member-query-interval
-> ipv6 multicast vlan 4 last-member-query-interval 2200
-> ipv6 multicast vlan 3-5 last-member-query-interval 2200
-> ipv6 multicast vlan 4 last-member-query-interval 0
-> no ipv6 multicast vlan 4 last-member-query-interval
-> ipv6 multicast vlan 3-5 last-member-query-interval
-> ipv6 multicast service 2 last-member-query-interval 2200
-> ipv6 multicast service 3-5 last-member-query-interval 2200
-> ipv6 multicast service 2 last-member-query-interval 0
-> no ipv6 multicast service 2 last-member-query-interval
-> no ipv6 multicast service 3-5 last-member-query-interval
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

`show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`  
- `alaIpmsConfigType`  
- `alaIpmsConfigAddressType`  
- `alaIpmsConfigValue`  
- `alaIpmsConfigLastMemberQueryInterval`
**ipv6 multicast query-response-interval**

Sets the MLD query response interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id] query-response-interval [milliseconds]
```

```
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id] query-response-interval
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. **This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.**
- `milliseconds` MLD query response interval in milliseconds. Valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>milliseconds</code></td>
<td>10000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IPv6 Multicast Switching and Routing must be enabled to set the MLD query response interval to use on the system and/or the specified VLANs or SPB services.
- If the MLD query response interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The MLD query response interval refers to the time period to reply to an MLD query message.
- Use the **no** form of this command to restore the MLD query response interval back to the default value (10000 milliseconds) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, `ipv6 multicast query-response-interval 0`).
Examples

- `ipv6 multicast query-response-interval 20000`
- `ipv6 multicast query-response-interval 0`
- `no ipv6 multicast query-response-interval`
- `ipv6 multicast vlan 2 query-response-interval 20000`
- `ipv6 multicast vlan 3-5 query-response-interval 20000`
- `ipv6 multicast vlan 2 query-response-interval 0`
- `no ipv6 multicast vlan 2 query-response-interval`
- `ipv6 multicast service 2 query-response-interval 300`
- `ipv6 multicast service 3-5 query-response-interval 300`
- `ipv6 multicast service 2 query-response-interval 0`
- `no ipv6 multicast service 2 query-response-interval`
- `no ipv6 multicast service 3-5 query-response-interval`

Release History

Release 7.1.1; command was introduced.
Release 8.4.1; service parameter added.

Related Commands

- `show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

- `alaIpmsConfigTable`
- `alaIpmsConfigType`
- `alaIpmsConfigAddressType`
- `alaIpmsConfigValue`
- `alaIpmsConfigQueryReponseInterval`
**ipv6 multicast unsolicited-report-interval**

Sets the value of the MLD unsolicited report interval on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] unsolicited-report-interval [seconds]
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] unsolicited-report-interval
```

### Syntax Definitions

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `seconds` MLD unsolicited report interval in seconds. Valid range is 1–65535, where 0 represents the default setting.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>1</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD unsolicited report interval to use on the system and/or the specified VLANs or SPB services.
- If the MLD unsolicited report interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- The unsolicited report interval refers to the time period to proxy any changed MLD membership state.
- Use the `no` form of this command to restore the MLD unsolicited report interval back to the default value (1 second) on the system, the specified VLAN, or the specified SPB service. In addition,
specifying a value of 0 with this command also restores the default value (for example, `ipv6 multicast unsolicited-report-interval 0`).

**Examples**

```
-> ipv6 multicast unsolicited-report-interval 20000
-> ipv6 multicast unsolicited-report-interval 0
-> no ipv6 multicast unsolicited-report-interval
-> ipv6 multicast vlan 2 unsolicited-report-interval 20000
-> ipv6 multicast vlan 3-5 unsolicited-report-interval 20000
-> ipv6 multicast vlan 2 unsolicited-report-interval 0
-> no ipv6 multicast vlan 2 unsolicited-report-interval
-> ipv6 multicast vlan 3-5 unsolicited-report-interval 0
-> no ipv6 multicast vlan 2 unsolicited-report-interval
-> ipv6 multicast service 2 unsolicited-report-interval 300
-> ipv6 multicast service 3-5 unsolicited-report-interval 300
-> ipv6 multicast service 2 unsolicited-report-interval 0
-> no ipv6 multicast service 2 unsolicited-report-interval
-> no ipv6 multicast service 3-5 unsolicited-report-interval
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

- `show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`  
  - `alaIpmsConfigType`  
  - `alaIpmsConfigAddressType`  
  - `alaIpmsConfigValue`  
  - `alaIpmsConfigUnsolicitedReportInterval`
ipv6 multicast router-timeout

Configures the expiry time of IPv6 multicast routers on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] router-timeout [seconds]

no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] router-timeout

Syntax Definitions

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **service_id[-service_id2]**: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **seconds**: MLD router timeout in seconds. Valid range is 1–65535.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>90</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD router timeout on the system and/or the specified VLANs. apply this configuration.
- If the MLD router timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- Use the no form of this command to restore the MLD router timeout back to the default value (90 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, ipv6 multicast router-timeout 0).

Examples

- -> ipv6 multicast router-timeout 100
- -> ipv6 multicast router-timeout 0
-> no ipv6 multicast router-timeout
-> ipv6 multicast vlan 2 router-timeout 100
-> ipv6 multicast vlan 3-5 router-timeout 100
-> ipv6 multicast vlan 2 router-timeout 0
-> no ipv6 multicast vlan 2 router-timeout
-> ipv6 multicast vlan 3-5 router-timeout
-> ipv6 multicast service 2 router-timeout 100
-> ipv6 multicast service 3-5 router-timeout 100
-> ipv6 multicast service 2 router-timeout 0
-> no ipv6 multicast service 2 router-timeout
-> no ipv6 multicast servicee 3-5 router-timeout

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R02; service parameter added.

**Related Commands**

- **show ipv6 multicast**
  Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- **alaIpmsConfigTable**
  - **alaIpmsConfigRouterTimeout**
ipv6 multicast source-timeout

Configures the expiry time of IPv6 multicast sources on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] source-timeout [seconds]
```

```
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] source-timeout
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `seconds` MLD source timeout in seconds. Valid range is 1–65535.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Is supported</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IPv6 Multicast Switching and Routing must be enabled to set the MLD source timeout on the system and/or the specified VLANs.
- If the MLD source timeout is already configured on the system, then the VLAN configuration will override the system's configuration.
- Use the `no` form of this command to restore the MLD source timeout back to the default value (30 seconds) on the system or the specified VLAN. In addition, specifying a value of 0 with this command also restores the default value (for example, `ipv6 multicast source-timeout 0`).

**Examples**

- `ipv6 multicast source-timeout 100`
- `ipv6 multicast source-timeout 0`
- `no ipv6 multicast source-timeout`
-> ipv6 multicast vlan 2 source-timeout 100
-> ipv6 multicast vlan 3-5 source-timeout 100
-> ipv6 multicast vlan 2 source-timeout 0
-> no ipv6 multicast vlan 2 source-timeout
-> no ipv6 multicast vlan 3-5 source-timeout 100
-> ipv6 multicast service 2 source-timeout 100
-> ipv6 multicast service 3-5 source-timeout 100
-> ipv6 multicast service 2 source-timeout 0
-> no ipv6 multicast service 2 source-timeout
-> no ipv6 multicast service 3-5 source-timeout

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1.R02; service parameter added.

**Related Commands**

**show ipv6 multicast** Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigSourceTimeout
ipv6 multicast querying

Enables or disables MLD querying on the specified VLAN or on the system if no VLAN is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2]] querying [{enable | disable}] [static-source-ip ipv6_address]
no ipv6 multicast [vlan vlan_id[-vlan_id2]] querying [static-source-ip]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `enable`: Enable MLD querying.
- `disable`: Disable MLD querying.
- `ipv6_address`: A static source IPv6 address to use for MLD querying. *This parameter is not supported.*

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- IPv6 Multicast Switching and Routing must be enabled to enable MLD querying on the system and/or specified VLANs.
- If the MLD querying is already enabled/disabled on the system, then the VLAN configuration will override the system's configuration.
- MLD querying refers to requesting the network's MLD group membership information by sending out MLD queries. MLD querying also involves participating in MLD querier election.
- Use the `no` form of this command to restore the MLD querying status to the default value (disabled) on the system or the specified VLAN.

**Examples**

```
-> ipv6 multicast querying enable
-> ipv6 multicast querying disable
```
-> no ipv6 multicast querying
-> ipv6 multicast vlan 2 querying enable
-> ipv6 multicast vlan 3-5 querying disable
-> no ipv6 multicast vlan 2 querying
-> no ipv6 multicast vlan 3-5 querying

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1.R02; static-source-ip parameter added.

**Related Commands**

*show ipv6 multicast*  Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigQuerying
  alaIpmsConfigQueryingStaticSourceAddress
**ipv6 multicast robustness**

Sets the MLD robustness variable on the specified VLAN, Shortest Path Bridging (SPB) service or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] robustness [robustness]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] robustness
```

### Syntax Definitions

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `robustness`: MLD robustness variable. Valid range is 1–7.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>robustness</td>
<td>2</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- IPv6 Multicast Switching and Routing must be enabled to set the MLD robustness variable on the system and/or the specified VLANs or SPB services.

- If the MLD robustness variable is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.

- Robustness variable allows fine-tuning on the network, where the expected packet loss would be greater.

- Due to protocol inter-operation requirements, this command specifies only a default version of the MLD robustness variable to use.
Use the **no** form of this command to restore the MLD robustness variable back to the default value (2) on the system, the specified VLAN, or the specified SPB service. In addition, specifying a value of 0 with this command also restores the default value (for example, `ipv6 multicast robustness 0`).

**Examples**

```
-> ipv6 multicast robustness 3
-> ipv6 multicast robustness 0
-> no ipv6 multicast robustness
-> ipv6 multicast vlan 2 robustness 3
-> ipv6 multicast vlan 3-5 robustness 3
-> ipv6 multicast vlan 2 robustness 0
-> no ipv6 multicast vlan 2 robustness
-> no ipv6 multicast vlan 3-5 robustness
-> ipv6 multicast service 2 robustness 3
-> ipv6 multicast service 3-5 robustness 3
-> ipv6 multicast service 2 robustness 0
-> ipv6 multicast service 2 robustness
-> no ipv6 multicast service 3-5 robustness
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; **service** parameter added.

**Related Commands**

- `show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigRobustness
ipv6 multicast spoofing

Enables or disables MLD spoofing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing {enable | disable}
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id] spoofing
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id[-vlan_id2]</code></td>
<td>VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.</td>
</tr>
<tr>
<td><code>service_id[-service_id2]</code></td>
<td>SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enable MLD spoofing.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disable MLD spoofing.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td></td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If the MLD spoofing is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD spoofing refers to replacing a client's MAC and IPv6 address with the system's MAC and IPv6 address when proxying aggregated MLD group membership information.
- By default, the source IPv6 address is not specified for spoofing; the system determines these addresses automatically. Optionally configure a static source IPv6 address to overcome the need for an IPv6 interface. If configured, the static source IPv6 is always used for spoofing, regardless of the IPv6 interface address or administrative state.
- Use the no form of this command to remove an MLD spoofing configuration and return the specified VLAN, SPB service, or system to the default behavior.
Examples

-> ipv6 multicast spoofing enable
-> ipv6 multicast spoofing disable
-> no ipv6 multicast spoofing
-> ipv6 multicast vlan 2 spoofing enable
-> ipv6 multicast vlan 3-5 spoofing disable
-> no ipv6 multicast vlan 2 spoofing
-> no ipv6 multicast vlan 3-5 spoofing
-> ipv6 multicast service 2 spoofing enable
-> ipv6 multicast service 3-5 spoofing disable
-> no ipv6 multicast service 2 spoofing
-> no ipv6 multicast service 3-5 spoofing

Release History

Release 7.1.1; command was introduced.
Release 8.4.1.R02; service parameter added.

Related Commands

show ipv6 multicast
Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigSpoofing
**ipv6 multicast spoofing static-source-ip**

Enables or disables MLD static spoofing on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing static-source-ip ipv6_address
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing static-source-ip
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`  
  VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.

- `service_id[-service_id2]`  
  SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

- `ipv6_address`  
  A static source IPv6 address to use for spoofing.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a static source IP address.
- MLD spoofing refers to replacing a client's MAC and IPv6 address with the system's MAC and IPv6 address when proxying aggregated MLD group membership information.
- By default, the source IPv6 address is not specified for spoofing; the system determines these addresses automatically. Optionally configure a static source IPv6 address to overcome the need for an IPv6 interface. If configured, the static source IPv6 is always used for spoofing, regardless of the IPv6 interface address or administrative state.

**Examples**

```
-> ipv6 multicast spoofing static-source-ip 3333::1
```
-> no ipv6 ip multicast spoofing static-source-ip
-> ipv6 multicast vlan 2 spoofing static-source-ip 3333::1
-> ipv6 multicast vlan 3-5 spoofing static-source-ip 3333::1
-> no ipv6 ip multicast vlan 2 spoofing static-source-ip
-> no ipv6 multicast vlan 3-5 spoofing static-source-ip
-> ipv6 multicast service 2 spoofing static-source-ip 3333::1
-> no ipv6 multicast service 2 spoofing static-source-ip
-> ipv6 multicast service 3-5 spoofing static-source-ip 3333::1
-> no ipv6 multicast service 3-5 spoofing static-source-ip

**Release History**

Release 8.3.1.R02; command was added.
Release 8.4.1.R02; service parameter added.

**Related Commands**

**show ipv6 multicast**
Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigSpoofing
alaIpmsConfigSpoofingStaticSourceAddress
**ipv6 multicast zapping**

Enables or disables MLD zapping on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zapping [enable | disable]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zapping
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` - VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` - SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable` - Enable MLD zapping.
- `disable` - Disable MLD zapping.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the MLD zapping is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD zapping refers to processing membership and source filter removals immediately and not waiting for the protocol's specified time period. This mode facilitates IP TV applications looking for quick changes between IP multicast groups.
- Use the no form of this command to restore the MLD zapping status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

**Examples**

```
-> ipv6 multicast zapping enable
```
-> ipv6 multicast zapping disable
-> no ipv6 multicast zapping
-> ipv6 multicast vlan 2 zapping enable
-> ipv6 multicast vlan 3-5 zapping disable
-> no ipv6 multicast vlan 2 zapping
-> no ipv6 multicast vlan 3-5 zapping
-> ipv6 multicast service 2 zapping enable
-> ipv6 multicast service 3-5 zapping disable
-> no ipv6 multicast service 2 zapping
-> no ip multicast service 3-5 zapping

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

`show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  - alaIpmsConfigType
  - alaIpmsConfigAddressType
  - alaIpmsConfigValue
  - alaIpmsConfigZapping
**ipv6 multicast querier-forwarding**

Enables or disables MLD querier forwarding on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querier-forwarding [enable | disable]
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querier-forwarding
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `enable`: Enable MLD querier forwarding.
- `disable`: Disable MLD querier forwarding.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the MLD querier forwarding is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD querier forwarding refers to promoting detected MLD queriers to receive all IP multicast data traffic.
- Use the `no` form of this command to restore the MLD querier forwarding status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.

**Examples**

```
-> ipv6 multicast querier-forwarding enable
```
-> ipv6 multicast querier-forwarding disable
-> no ipv6 multicast querier-forwarding
-> ipv6 multicast vlan 2 querier-forwarding enable
-> ipv6 multicast vlan 3-5 querier-forwarding disable
-> no ipv6 multicast vlan 2 querier-forwarding
-> no ipv6 multicast vlan 3-5 querier-forwarding
-> ipv6 multicast service 2 querier-forwarding enable
-> ipv6 multicast service 3-5 querier-forwarding disable
-> no ipv6 multicast service 2 querier-forwarding
-> no ipv6 multicast service 3-5 querier-forwarding

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; *service* parameter added.

**Related Commands**

`show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigQuerierForwarding
**ipv6 multicast proxying**

Enables or disables MLD proxying on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying [enable | disable]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `enable` Enable MLD proxying.
- `disable` Disable MLD proxying.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the MLD proxying is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.
- MLD proxying refers to processing membership information on behalf of client systems and reporting membership on their behalf.
- Proxy reported MLD packets are sent using the source MAC address of the proxying switch. Unless the spoofing feature is used, proxy reported MLD packets will be sent using “::” for the IPv6 source address.
- Use the `no` form of this command to restore the MLD proxying status back to the default value (disabled) on the system, the specified VLAN, or the specified SPB service.
**Examples**

- `ipv6 multicast proxying enable`
- `ipv6 multicast proxying disable`
- `no ipv6 multicast proxying`
- `ipv6 multicast vlan 2 proxying enable`
- `ipv6 multicast vlan 3-5 proxying disable`
- `no ipv6 multicast vlan 2 proxying`
- `ipv6 multicast vlan 3-5 proxying`
- `ipv6 multicast service 2 proxying enable`
- `ipv6 multicast service 3-5 proxying disable`
- `no ipv6 multicast service 2 proxying`
- `no ipv6 multicast service 3-5 proxying`

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; `service` parameter added.

**Related Commands**

- `show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigProxying`
ipv6 multicast helper-address

Specifies the destination IPv6 address of a relay host where MLD host Reports and Leave messages are sent.

```
ipv6 multicast [vlan vlan_id[-vlan_id2]] helper-address [ipv6_address]
no ipv6 multicast [vlan vlan_id[-vlan_id2]] helper-address
```

### Syntax Definitions

- `vlan_id[=vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `ipv6_address` The IPv6 address of the relay host.

### Defaults

By default, no destination IPv6 address is set.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- After the destination IPv6 address is specified, the IPMS reporting feature is enabled.
- An operational IPv6 interface is required for the receiving LAN before any MLD Reports and Leave messages can be relayed.
- Configuring a destination IPv6 helper address is supported only in the VLAN domain; the service domain is not supported.
- Use the `no` form of this command to restore the IPMS reporting feature back to the default value (no IPv6 helper address) on the system. When there is no IPv6 helper address set, the IPMS reporting feature is disabled.

### Examples

```
-> ipv6 multicast helper-address 3333::2
-> no ipv6 multicast helper-address
-> ipv6 multicast vlan 2 helper-address 3333::2
-> ipv6 multicast vlan 3-5 helper-address 3333::2
-> no ipv6 multicast vlan 2 helper-address
-> no ipv6 multicast vlan 3-5 helper-address
```
**Release History**

Release 8.4.1; command was introduced.
Release 8.4.1.R02; **vlan** parameter added.

**Related Commands**

- `show ipv6 multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigHelperAddress`
ipv6 multicast zero-based-query

Configures the use of an all-zero source IPv6 address for MLD query packets when a non-querier is querying the membership of a port. This value is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query [enable | disable]
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query
```

### Syntax Definitions

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable` Enable MLD zero-based querying.
- `disable` Disable MLD zero-based querying.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The MLD zero-based query status set for a specific VLAN or SPB service overrides the zero-based query status set for the system.
- Use the `no` form of this command to restore the MLD zero-based query status back to the default value (enabled) on the system, the specified VLAN, or the specified SPB service.

### Examples

- `ipv6 multicast zero-based-query enable`
- `ipv6 multicast zero-based-query disable`
- `no ipv6 multicast zero-based-query`
-> ipv6 multicast vlan 2 zero-based-query enable
-> ipv6 multicast vlan 3-5 zero-based-query disable
-> no ipv6 multicast vlan 2 zero-based-query
-> no ipv6 multicast vlan 3-5 zero-based-query
-> ipv6 multicast service 10 zero-based-query enable
-> ipv6 multicast service 11-15 zero-based-query disable
-> no ipv6 multicast service 10 zero-based-query
-> no ipv6 multicast service 11-15 zero-based-query disable

**Release History**

Release 8.3.1; command introduced.
Release 8.4.1; service parameter added.

**Related Commands**

*show ipv6 multicast* Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigZeroBasedQuery
**ipv6 multicast forward-mode**

Configures the Layer 2 forwarding mode for IPv6 Multicast Switching (does not apply to IPv6 Multicast Routing). The forwarding mode is set for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] forward-mode {asm | ssm | mac | auto}
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] forward-mode
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` - VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` - SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `asm` - Sets the IPMSv6 forwarding mode to ASM (the bridge lookup is based on the packet group destination IPv6 address). This parameter is supported only in the VLAN domain; service domain is not supported.
- `ssm` - Sets the IPMSv6 forwarding mode to SSM (the bridge lookup is based on the packet source IPv6 as well as the group destination IPv6). This parameter is supported only in the VLAN domain; service domain is not supported.
- `mac` - Sets the IPMSv6 forwarding mode to MAC address (the bridge lookup is based on the MAC destination address).
- `auto` - Automatically determines the IPMSv6 forwarding mode based on the current MLD protocol version and the existing protocol state.

**Defaults**

By default, the forwarding mode is set to automatic.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- The forwarding mode set for a specific VLAN or SPB service overrides the forwarding mode set for the system.

- If multicast routing is enabled on a VLAN, the following conditions apply:
  - On the OmniSwitch 9900, the bridging mode is independent of the routing mode. As a result, ASM bridging is allowed in a VLAN that has SSM routing configured or SSM bridging is allowed in a VLAN that has ASM routing configured.
  - Multicast routing is not supported on the OmniSwitch 6560 and OmniSwitch 6570M.
  - On all other OmniSwitch platforms, the routing configuration overrides the forwarding mode setting and determines the forwarding mode based on the group mappings. For example, BIDIR flows will use ASM while DVMRP flows and all other PIM modes will use SSM.

- Use the no form of this command to restore the Layer 2 forwarding mode back to the default value (automatic) on the system, the specified VLAN or SPB service.

Examples

```
-> ipv6 multicast forward-mode auto
-> ipv6 multicast forward-mode asm
-> ipv6 multicast forward-mode ssm
-> ipv6 multicast forward-mode mac
-> no ipv6 multicast forward-mode
-> ipv6 multicast vlan 100 forward-mode auto
-> ipv6 multicast vlan 101-104 forward-mode asm
-> ipv6 multicast vlan 100 forward-mode ssm
-> ipv6 multicast vlan 101-104 forward-mode mac
-> no ipv6 multicast vlan 100 forward-mode
-> no ipv6 multicast vlan 101-104 forward-mode
-> ipv6 multicast service 10 forward-mode mac
-> ipv6 multicast service 11-15 forward-mode mac
-> no ipv6 multicast service 10 forward-mode
-> no ipv6 multicast service 11-15 forward-mode
```

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; service parameter added.

Related Commands

- **show ipv6 multicast** Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.
- **show ipv6 multicast bridge** Displays IPv6 multicast bridge table entries.

MIB Objects

- `alaIpmsConfigTable`
  - `alaIpmsConfigType`
  - `alaIpmsConfigAddressType`
  - `alaIpmsConfigValue`
  - `alaIpmsConfigForwardMode`
**ipv6 multicast update-delay-interval**

Sets the amount of time to delay IPv6 multicast forwarding updates on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

**Syntax**

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval milliseconds
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]` SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `milliseconds` The number of milliseconds to defer forwarding updates. Valid range is 0–10000.

**Defaults**

By default, the forwarding update delay interval is set to zero.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the forwarding update delay is set to zero, forwarding updates are processed immediately with minimal latency. Configuring a forwarding update delay value can limit the effects of persistent churn on the system.
- If the forwarding update delay interval is already configured on the system, then the VLAN or SPB service configuration will override the system's configuration.
- Use the `no` form of this command to restore the forwarding update delay interval back to the default value (zero) on the system or the specified VLAN or SPB service.

**Examples**

```
-> ipv6 multicast update-delay-interval 10
-> no ipv6 multicast update-delay-interval
```
-> ipv6 multicast vlan 100 update-delay-interval 20  
-> ipv6 multicast vlan 101-105 update-delay-interval 20  
-> no ipv6 multicast vlan 100 update-delay-interval 20  
-> no ipv6 multicast vlan 101-105 update-delay-interval  
-> ipv6 multicast service 20 update-delay-interval 20  
-> ipv6 multicast service 21-25 update-delay-interval 20  
-> no ipv6 multicast service 20 update-delay-interval  
-> no ipv6 multicast service 21-25 update-delay-interval

**Release History**
Release 8.3.1; command was introduced.  
Release 8.4.1.R02; service parameter added.

**Related Commands**

*show ipv6 multicast* Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**
alaIpmsConfigTable  
alaIpmsConfigType  
alaIpmsConfigAddressType  
alaIpmsConfigValue  
alaIpmsConfigUpdateDelayInterval
ipv6 multicast fast-join

Configures whether or not IPv6 Multicast Switching will automatically create the forwarding entries in hardware as soon as the MLD memberships are learned on the specified VLAN, Shortest Path Bridging (SPB) service or globally if no VLAN or SPB service is specified.

```
ipv6 multicast [vlan vlan_id[vlan_id2] | service service_id[service_id2]] fast-join [enable | disable]
no ipv6 multicast [vlan vlan_id[vlan_id2] | service service_id[service_id2]] fast-join
```

Syntax Definitions

- `vlan_id[vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs. *This parameter is supported only on the OmniSwitch 9900.*
- `service_id[service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `enable`: Enable the MLD fast join functionality.
- `disable`: Disable the MLD fast join functionality.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command applies only to IPv6 Multicast Switching. If IPv6 Multicast Routing is enabled, then the routing configuration will override the fast join setting.
- When the IPv6 Multicast Switching fast join functionality is enabled, convergence of multicast traffic may occur faster because the forwarding entries are already created before the actual multicast traffic is received.
- When the IPv6 Multicast Switching fast join functionality is disabled (the default), forwarding entries are not created in the hardware until the multicast traffic reaches the switch.
• If the IPv6 Multicast Switching fast join is already enabled on the system, then the VLAN or SPB service configuration will override the system's configuration.

• Use the no form of this command to restore the IPv6 Multicast Switching fast join setting back to the default value (disabled) on the system or the specified VLAN or SPB service.

**Examples**

-> ipv6 multicast fast-join enable
-> ipv6 multicast fast-join disable
-> no ipv6 multicast fast-join
-> ip multicast service 10 fast-join enable
-> ip multicast service 11-15 fast-join disable
-> no ip multicast service 10 fast-join
-> no ip multicast service 11-15 fast-join

**Release History**

Release 8.3.1.R02; command introduced.
Release 8.4.1.R02; vlan and service parameters added.

**Related Commands**

`show ip multicast` Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

**MIB Objects**

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigFastJoin
**ipv6 multicast host-list**

Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

```
ipv6 multicast host-list host_list_name ipv6_address [ipv6_address]
```

```
no ipv6 multicast host-list host_list_name [ipv6_address]
```

**Syntax Definitions**

- `host_list_name`: A name to assign to the host list (up to 20 characters).
- `ipv6_address`: The IPv6 address to add to the host list. Multiple IPv6 addresses can be entered on the same command line.

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- Use the `no` form of this command to remove an IPv6 address from the list or remove the entire list from the switch configuration.
- When the entire list is removed, any configuration associated with the list is also removed.

**Examples**

```
-> ipv6 multicast host-list group-map1 4444::2
-> ipv6 multicast host-list ssm-map1 4444::3
-> ipv6 multicast host-list ssm-map2 3333::2 3333::3 3333::4
-> no ipv6 multicast host-list ssm-map2 3333::3
-> no ipv6 multicast host-list group-map1
```

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

- `show ipv6 multicast host-list`: Displays the IPv6 multicast host address list configuration.

**MIB Objects**

- `alaIpmsHostListTable`  
  - `alaIpmsHostListName`  
  - `alaIpmsHostListAddressType`  
  - `alaIpmsHostListAddress`
### ipv6 multicast ssm-map

Configures the translation of Any Source Multicast (ASM) group memberships into Source Specific Multicast (SSM) group memberships on the specified VLAN or on the system if no VLAN is specified.

```plaintext
ipv6 multicast [vlan vlan_id] ssm-map {group_address[/prefixLen] host_list_name | admin-state {enable | disable}}

no ipv6 multicast ssm-map group_address[/prefixLen]
```

#### Syntax Definitions

- **vlan_id**: VLAN on which to apply the mapping configuration.
- **group_address[/prefixLen]**: The multicast group address/prefix length to map to the host list. If no prefix length is specified, then the default length of 128 is used.
- **host_list_name**: The name of a host list to use for SSM mapping.
- **enable**: Enables the SSM mapping.
- **disable**: Disables the SSM mapping.

#### Defaults

N/A

#### Platforms Supported

Not supported in this release.

#### Usage Guidelines

- Use the `no` form of this command to remove the SSM mapping configuration.
- If an SSM mapping is already enabled on the system, then the VLAN configuration will override the system's configuration.

#### Examples

- `-> ipv6 multicast ssm-map ff05::5 hostList1`
- `-> ipv6 multicast ssm-map admin-state enable`
- `-> ipv6 multicast vlan 200 ssm-map ff05::6 hostList2`
- `-> ipv6 multicast vlan 200 ssm-map admin-state enable`
- `-> no ipv6 multicast ssm-map ff05::5`

#### Release History

Release 8.3.1.R02; command was introduced.
**Related Commands**

- `show ipv6 multicast ssm-map`  
  Displays the SSM mapping configuration.

- `show ipv6 multicast`  
  Displays the IPv6 Multicast Switching and Routing status and general configuration parameters, such as the global SSM mapping setting.

**MIB Objects**

- `alaIpmsSsmMapTable`
- `alaIpmsSsmMapConfigType`
- `alaIpmsSsmMapConfigAddressType`
- `alaIpmsSsmMapConfigValue`
- `alaIpmsSsmMapGroupAddress`
- `alaIpmsSsmMapGroupPrefixLength`
- `alaIpmsSsmMapSourceListName`
**ipv6 multicast initial-packet-buffer admin-state**

Enables or disables initial packet buffering for IPv6 multicast flows on the specified VLAN or globally on the switch.

```
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer admin-state {enable | disable}
```

### Syntax Definitions

`vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.

`enable` Enable the initial packet buffering globally on the switch for IPv6 multicast flow.

`disable` Disable the initial packet buffering globally on the switch for IPv6 multicast flow.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When enabled, the following configuration is used for initial packet buffering on new multicast flows:
  - The maximum number of initial packets buffered per IPv6 multicast flow. Use the `ipv6 multicast initial-packet-buffer max-packet` command to set this value.
  - The maximum number of IPv6 multicast flows that can be buffered. Use the `ipv6 multicast initial-packet-buffer max-flow` command to set this value.
  - The maximum amount of time buffered packets are held if they are not sent out. Use the `ipv6 multicast initial-packet-buffer timeout` command to set this value.
  - The minimum amount of time packets are held before delivery begins. Use the `ipv6 multicast initial-packet-buffer min-delay` command to set this value.
- Configuring the status for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.
**Examples**

-> ipv6 multicast initial-packet-buffer admin-state disable
-> ipv6 multicast initial-packet-buffer admin-state enable
-> ipv6 multicast vlan 2 initial-packet-buffer admin-state enable
-> ipv6 multicast vlan 3-5 initial-packet-buffer admin-state enable

**Release History**

Release 8.2.1; command introduced.
Release 8.4.1.R02; `vlan` parameter added.

**Related Commands**

`show ipv6 multicast` Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

**MIB Objects**

alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBuffer
**ipv6 multicast initial-packet-buffer max-packet**

Configures the maximum number of initial packets buffered per IPv6 multicast flow on the specified VLAN or globally on the switch.

```
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer max-packet [num]
```

---

### Syntax Definitions

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **num**: The maximum number of packets allowed to buffer per IPv6 multicast flow. Valid range is 1 to 10.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>4</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

### Examples

- `ipv6 multicast initial-packet-buffer max-packet 4`
- `ipv6 multicast vlan 2 initial-packet-buffer max-packet 10`
- `ipv6 multicast vlan 3-5 initial-packet-buffer max-packet 10`

### Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; `vlan` parameter added.
**Related Commands**

- `ipv6 multicast initial-packet-buffer admin-state` Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.
- `show ipv6 multicast` Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

**MIB Objects**

- `alaIpmsConfigTable`
- `alaIpmsConfigType`
- `alaIpmsConfigAddressType`
- `alaIpmsConfigValue`
- `alaIpmsConfigInitialPacketBufferMaxPacket`
**ipv6 multicast initial-packet-buffer max-flow**

Configures the maximum number of IPv6 multicast flows that can be buffered on the specified VLAN or globally on the switch.

```
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer max-flow [num]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `num` The maximum number of IPv6 multicast flows allowed for initial packet buffering. Valid range is 1 to 32.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>num</code></td>
<td>32</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

**Examples**

- `ipv6 multicast initial-packet-buffer max-flow 32`
- `ipv6 multicast vlan 2 initial-packet-buffer max-flow 32`
- `ipv6 multicast vlan 3-5 initial-packet-buffer max-flow 32`

**Release History**

Release 8.2.1; command introduced.
Release 8.4.1.R02; `vlan` parameter added.
**Related Commands**

`ipv6 multicast initial-packet-buffer admin-state`  
Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.

`show ip multicast`  
Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

**MIB Objects**

`alaIpmsConfigTable`
- `alaIpmsConfigType`
- `alaIpmsConfigAddressType`
- `alaIpmsConfigValue`
- `alaIpmsConfigInitialPacketBufferMaxFlow`
ipv6 multicast initial-packet-buffer timeout

Configures the timeout value for the buffered IPv6 initial multicast packets on the specified VLAN or globally on the switch.

ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer timeout [seconds]

**Syntax Definitions**

- **vlan_id[-vlan_id2]**: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- **seconds**: The timeout value for the initial buffered IPv6 multicast packets in seconds. Valid range is 1 to 10.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>10</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the buffered multicast packet is not sent out before the timeout, then the buffered packets will be removed from IPMS system.
- The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.
- Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

**Examples**

- `ipv6 multicast initial-packet-buffer timeout 2`
- `ipv6 multicast vlan 2 initial-packet-buffer timeout 5`
- `ipv6 multicast vlan 3-5 initial-packet-buffer timeout t`

**Release History**

Release 8.2.1; command introduced.
Release 8.4.1.R02; **vlan** parameter added.
Related Commands

**ipv6 multicast initial-packet-buffer admin-state**
Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.

**show ip multicast**
Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

MIB Objects

alaIpmsConfigTable
alaIpmsConfigType
alaIpmsConfigAddressType
alaIpmsConfigValue
alaIpmsConfigInitialPacketBufferTimeout
ipv6 multicast initial-packet-buffer min-delay

Configures the minimum delay to program the multicast replication index for IPv6 multicast flows buffered for initial packet on the specified VLAN or globally on the switch.

ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer min-delay [milliseconds]

Syntax Definitions

vlan_id[-vlan_id2] VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
milliseconds The minimum delay value to program the multicast replication index for IPv6 multicast flows buffered for initial packet. Valid range is 0 to 1000.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliseconds</td>
<td>0</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Note. This command configures a timer to delay the programming of multicast replication index in hardware which might increase the number of multicast packets lost during the learning phase.

• The configuration value set with this command is not applied unless initial packet buffering is administratively enabled for the switch.

• Configuring parameter values for initial packet buffering is supported only in the VLAN domain; the service domain is not supported.

Examples

-> ipv6 multicast initial-packet-buffer min-delay 200
-> ipv6 multicast vlan 2 initial-packet-buffer min-delay 200
-> ipv6 multicast vlan 3-5 initial-packet-buffer min-delay 200
Release History

Release 8.2.1; command introduced.
Release 8.4.1.R02; vlan parameter added.

Related Commands

ipv6 multicast initial-packet-buffer admin-state
Enables or disables the initial packet buffering feature globally on the switch for IPv6 multicast flows.

show ip multicast
Displays the status and configuration parameters of initial multicast packet buffer for IPv6 flows on the switch.

MIB Objects

alaIpmsConfigTable
   alaIpmsConfigType
   alaIpmsConfigAddressType
   alaIpmsConfigValue
   alaIpmsConfigInitialPacketBufferMinDelay
ipv6 multicast display-interface-names

Sets the display output of the show commands listed below. When enabled, the display outputs for these commands will show the IPv6 interface name for each VLAN associated with the IPv6 multicast table entry.

**ipv6 multicast display-interface-names**

**no ipv6 multicast display-interface-names**

---

**Syntax Definitions**

N/A

**Defaults**

By default, this function is disabled. The display format is set to include the VLANs that are associated with the IPv6 multicast source and forward flows.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the no form of this command to revert back to displaying the VLAN name.
- If there are any VLANs that are not configured with an IPv6 interface or the IPv6 interface is disabled, the output display will still include the VLAN when this function is enabled.
- This command may be helpful when reviewing output from multicast snooping commands and comparing state in multicast routing, which only interacts with IPv6 interfaces.
- Enabling the display interface names option applies to the following show commands:
  - `show ipv6 multicast forward`
  - `show ipv6 multicast neighbor`
  - `show ipv6 multicast querier`
  - `show ipv6 multicast group`
  - `show ipv6 multicast source`
  - `show ipv6 multicast tunnel`
- The command examples provided display the show ipv6 multicast source output after the display interface name function is turned on (enabled) and off (disabled).
**Examples**

-> ipv6 multicast display-interface-name

-> show ipv6 multicast source

Total 4 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::5</td>
<td>4444::2</td>
<td>::</td>
<td>VL-21</td>
</tr>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>VL-21</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>VL-20</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>VL-20</td>
</tr>
</tbody>
</table>

-> no ip multicast display-interface-name

-> show ipv6 multicast source

Total 4 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::5</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 21</td>
</tr>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 21</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

- `show ipv6 multicast source` Displays the IPv6 Multicast Switching and Routing source table entries.
- `show ipv6 multicast forward` Displays the IPv6 Multicast Switching and Routing forwarding table entries.

**MIB Objects**

alaIpmsGlobalConfigTable
  alaIpmsGlobalConfigAddressType
  alaIpmsGlobalConfigDisplayInterfaceNames
**ipv6 multicast inherit-default-vrf-config**

Configures whether or not the global IPMSv6 configuration defined in the default VRF instance is applied to all VRF instances.

```plaintext
ipv6 multicast inherit-default-vrf-config

no ipv6 multicast inherit-default-vrf-config
```

**Syntax Definitions**

N/A

**Defaults**

By default, the global IPMSv6 configuration defined in the default VRF instance is applied to all VRF instances on the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable this function. When disabled, the global IPMSv6 configuration defined in the default VRF instance is not applied to all other VRF instances on the switch.

- When enabled, additional VRF instances will inherit the global IPMSv6 configuration defined in the default VRF instance.

- A global IPMSv6 configuration defined for a specific non-default VRF instance takes precedence over the global IPMSv6 configuration defined for the default VRF.

**Examples**

- `ipv6 multicast inherit-default-vrf-config`
- `no ipv6 multicast inherit-default-vrf-config`

**Release History**

Release 8.3.1; command introduced.
Related Commands

**show ipv6 multicast**  
Displays the IPv6 Multicast Switching and Routing status and general configuration parameters.

MIB Objects

`alaIpmsGlobalConfigTable`  
`alaIpmsGlobalConfigAddressType`  
`alaIpmsGlobalConfigInheritDefaultVrfConfig`
**ipv6 multicast profile**

Defines an IPMS profile that is used to apply a pre-defined configuration to the global IPMS instance (all VLAN and service instances) or to a specific VLAN or service instance. Using a configuration profile to configure IPMS functionality avoids having to configure each IPMS parameter with a separate CLI command.

This section describes the base command (`ipv6 multicast profile`) along with optional command keywords that are used to configure IPMS parameter values that are applied when the profile is assigned to an IPMS instance. Optional keywords are listed separately but can be entered in combination on the same command line. Use the `no` form for the keywords to change a specific parameter value for the profile.

There is a “default” profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance. The default profile cannot be deleted, but the profile parameter values are configurable through this command.

```
ipv6 multicast profile profile_name
  [admin-state {enable | disable}]
  [flood-unknown {enable | disable}]
  [version version]
  [robustness robustness]
  [querying {enable | disable}]
  [query-interval [seconds]]
  [query-response-interval [milliseconds]]
  [last-member-query-interval [milliseconds]]
  [unsolicited-report-interval [seconds]]
  [proxying {enable | disable}]
  [spoofing {enable | disable}]
  [spoofing static-source-ip ipv6_address]
  [zapping {enable | disable}]
  [querier-forwarding {enable | disable}]
  [router-timeout [seconds]]
  [source-timeout [seconds]]
  [max-group [num] [action {none | drop | replace}]]
  [helper-address [ipv6_address]]
  [zero-based-query {enable | disable}]
  [forward-mode {asm | ssm | mac | auto}]
  [update-delay-interval milliseconds]
  [fast-join {enable | disable}]
  [initial-packet-buffer admin-state {enable | disable}]
  [initial-packet-buffer max-flow [num]]
  [initial-packet-buffer max-packet [num]]
  [initial-packet-buffer timeout [seconds]]
  [initial-packet-buffer min-delay [milliseconds]]
```

```
no ipv6 multicast profile profile_name [admin-state | flood-unknown | version | robustness | ...]
```
**Syntax Definitions**

*profile_name* 

The name to associate with the IPMS profile.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to remove an IPMS profile from the switch configuration.
- To change the value of a specific profile parameter, specify the parameter keyword with this command. For example, *no ipv6 multicast profile ipms-1 admin-state*, *ipv6 multicast profile ipms-1 query-interval 100*, or *ipv6 multicast profile ipms-1 querying enable*. The new parameter values are applied to all IPMS instances to which the profile is assigned.
- The profile name must already exist in the switch configuration before parameter values can be modified. Use this command to create the profile first, then configure the profile parameter values.
- For more information about specific profile parameter values, refer to the following explicit IPMS configuration commands for each profile parameter:

<table>
<thead>
<tr>
<th>Port Template Parameter</th>
<th>Explicit Port Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>[admin-state {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[flood-unknown {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[version version]</td>
<td>ipv6 multicast version</td>
</tr>
<tr>
<td>[robustness robustness]</td>
<td>ipv6 multicast robustness</td>
</tr>
<tr>
<td>[querying {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[query-interval {seconds}]</td>
<td>ipv6 multicast query-interval</td>
</tr>
<tr>
<td>[query-response-interval [milliseconds]]</td>
<td>ipv6 multicast query-response-interval</td>
</tr>
<tr>
<td>[last-member-query-interval [milliseconds]]</td>
<td>ipv6 multicast last-member-query-interval</td>
</tr>
<tr>
<td>[unsolicited-report-interval {seconds}]</td>
<td>ipv6 multicast unsolicited-report-interval</td>
</tr>
<tr>
<td>[proxying {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[spoofing {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[spoofing static-source-ip ipv6_address]</td>
<td>ipv6 multicast spoofing static-source-ip</td>
</tr>
</tbody>
</table>
### Examples

- `ipv6 multicast profile “MLDv2 with Zapping”`
- `ipv6 multicast profile “MLDv2 with Zapping” admin-state enable`
- `ipv6 multicast profile “MLDv2 with Zapping” zapping enable version 2`
- `ipv6 multicast profile “MLDv2 with Zapping” fast-join enable proxying enable`
- `no ipv6 multicast profile “MLDv2 with Zapping” proxying`
- `no ipv6 multicast profile “MLDv2 with Zapping”`

### Release History

Release 8.4.1.R02; command was introduced.

### Related Commands

- **ipv6 multicast apply-profile**: Assigns an IPMS configuration profile globally for the switch or to a specific VLAN or service instance.
- **show ipv6 multicast**: Displays the profile assignment for the IPMS instance.
- **show ipv6 multicast profile**: Displays the IPMS profile configuration.
**MIB Objects**

alaIpmsProfileTable
- alaIpmsProfileAddressType
- alaIpmsProfileName
- alaIpmsProfileIndex
- alaIpmsProfileRowStatus

alaIpmsConfigTable
- alaIpmsConfigType
- alaIpmsConfigAddressType
- alaIpmsConfigValue
- alaIpmsConfigProfileName
**ipv6 multicast apply-profile**

Assigns the name of an existing IPMS configuration profile to the global IPMS instance (all VLANs and services) or to a specific VLAN or Shortest Path Bridging (SPB) service instance. An IPMS configuration profile defines parameter options that are applied to the IPMS instance to which the profile is assigned.

```
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] apply-profile profile_name
```

```
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] apply-profile
```

**Syntax Definitions**

- `vlan vlan_id[-vlan_id2]`: VLAN on which to apply the configuration. Use a hyphen to specify a range of VLAN IDs.
- `service_id[-service_id2]`: SPB service ID on which to apply the configuration. The valid range is 1–32767. Use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `profile_name`: The name to associate with the IPMS profile.

**Defaults**

There is a “default” profile that defines a default set of IPMS parameter values that is automatically assigned to an IPMS instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to revert the profile assignment back to the “default” profile.
- Specify a range of VLANs (`vlan 20-25`) or a range of SPB services (`service 10-15`) to apply the specified profile to multiple VLANs or services with one CLI command.
- The specified profile name must already exist in the switch configuration.

**Examples**

- `ipv6 multicast apply-profile “MLDv2 with Zapping”`
- `ipv6 multicast vlan 20 apply-profile “MLDv2 with Zapping”`
- `ipv6 multicast vlan 20-25 apply-profile “MLDv2 with Zapping”`
- `ipv6 multicast service 10 apply-profile “MLDv2 with Zapping”`
- `ipv6 multicast service 10-15 apply-profile “MLDv2 with Zapping”`
- `no ipv6 multicast apply-profile`
-> no ipv6 multicast vlan 20 apply-profile
-> no ipv6 multicast vlan 20-15 apply-profile
-> no ipv6 multicast service 10 apply-profile
-> no ipv6 multicast service 10-15 apply-profile

**Release History**

Release 8.4.1.R02; command was introduced.

**Related Commands**

- **ipv6 multicast profile**
  
  Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.

- **show ipv6 multicast**
  
  Displays the profile assignment for the IPMS instance.

- **show ipv6 multicast profile**
  
  Displays the IPMS profile configuration.

**MIB Objects**

- **alaIpmsProfileTable**
  
  - alaIpmsProfileAddressType
  - alaIpmsProfileName
  - alaIpmsProfileIndex
  - alaIpmsProfileRowStatus

- **alaIpmsConfigTable**
  
  - alaIpmsConfigType
  - alaIpmsConfigAddressType
  - alaIpmsConfigValue
  - alaIpmsConfigProfileName
**show ip multicast**

Displays the IP Multicast Switching and Routing status and the general configuration parameters for the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

```
show ip multicast [vlan vlan_id | service service_id]
```

**Syntax Definitions**

- `vlan_id`  
  VLAN ID number (1–4094).

- `service_id`  
  SPB service ID number (1–32767). *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

**Defaults**

By default the status and general configuration parameters for the system are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify a VLAN ID to display the configuration information for a specific VLAN.
- Specify an SPB service ID to display the configuration information for a specific SPB service.

**Examples**

```
-> show ip multicast

Profile                                          = default,
Status                                           = disabled,
Flood Unknown                                    = disabled,
Version                                          = 2,
Robustness                                       = 2,
Querying                                         = disabled,
Query Interval (seconds)                         = 125,
Query Response Interval (tenths of seconds)      = 100,
Last Member Query Interval (tenths of seconds)   = 10,
Unsolicited Report Interval (seconds)            = 1,
Proxying                                         = disabled,
Spoofing                                         = disabled,
Zapping                                          = disabled,
```
Querier Forwarding = disabled,
Router Timeout (seconds) = 90,
Source Timeout (seconds) = 30,
Max-group = 0,
Max-group action = none,
Helper-address = 0.0.0.0,
Static Querier Address = 0.0.0.0,
Static Spoofer Address = 0.0.0.0,
Zero-based Query = enabled,
Forward Mode = auto,
Update Delay Interval (milliseconds) = 0,
SSM Mapping = disabled,
Fast Join
Initial Packet Buffering
Max Flows = 32,
Max Packets Per Flow = 4,
Buffer Timeout (seconds) = 10,
Min Delay (milliseconds) = 0

-> show ip multicast vlan 200
Profile = default,
Status = disabled,
Flood Unknown = disabled,
Version = 2,
Robustness = 2,
Querying = disabled,
Query Interval (seconds) = 125,
Query Response Interval (tenths of seconds) = 100,
Last Member Query Interval (tenths of seconds) = 10,
Unsolicited Report Interval (seconds) = 1,
Proxying = disabled,
Spoofing = disabled,
Zapping = disabled,
Querier Forwarding = disabled,
Router Timeout (seconds) = 90,
Source Timeout (seconds) = 30,
Max-group = 0,
Max-group action = none,
Helper-address = 0.0.0.0,
Static Querier Address = 0.0.0.0,
Static Spoofer Address = 0.0.0.0,
Zero-based Query = disabled,
Forward Mode = auto,
Update Delay Interval (milliseconds) = 0,
SSM Mapping = disabled,
Fast Join
Initial Packet Buffering
Max Flows = 32,
Max Packets Per Flow = 32,
Buffer Timeout (seconds) = 10,
Min Delay (milliseconds) = 0

-> show ip multicast service 20
Profile = default,
Status = disabled,
Flood Unknown = disabled,
Version = 2,
Robustness = 2,
Querying = disabled,
Query Interval (seconds) = 125,
Query Response Interval (tenths of seconds) = 100,
Last Member Query Interval (tenths of seconds) = 10,
Unsolicited Report Interval (seconds) = 1,
Proxying = disabled,
Spoofing = disabled,
Zapping = disabled,
Querier Forwarding = disabled,
Router Timeout (seconds) = 0,
Source Timeout (seconds) = 300,
Max-group = 0,
Max-group action = none,
Helper-address = 0.0.0.0,
Static Querier Address = 0.0.0.0,
Static Spoofier Address = 0.0.0.0,
Zero-based Query = disabled,
Forward Mode = mac,
Update Delay Interval (milliseconds) = 0,
SSM Mapping = disabled,
Fast Join = disabled,
Initial Packet Buffering = disabled,
Max Flows = 32,
Max Packets Per Flow = 32,
Buffer Timeout (seconds) = 10,
Min Delay (milliseconds) = 0

output definitions

**Profile**
The name of a predefined IPMS configuration profile that is assigned to this instance. Configured through the `ip multicast profile` command.

**Status**
Whether IP Multicast Switching and Routing is **Enabled** or **Disabled** (the default status). Configured through the `ip multicast admin-state` command.

**Flood Unknown**
Whether the flooding of initial unknown multicast traffic is **Enabled** or **Disabled** (the default status). Configured through the `ip multicast flood-unknown` command.

**Version**
Displays the default IGMP version, which can be 1, 2 or 3. Configured through the `ip multicast version` command.

**Robustness**
Displays the IGMP robustness value, ranging from 1 to 7. (The default value is 2). Configured through the `ip multicast robustness` command.

**Querying**
Whether IGMP querying is **Enabled** or **Disabled** (the default status). Configured through the `ip multicast querying` command.

**Query Interval (seconds)**
Displays the time (in seconds) between IGMP queries. (The default value is 125 seconds). Configured through the `ip multicast query-interval` command.

**Query Response Interval (tenths of seconds)**
Displays the time (in tenths of seconds) taken to reply to an IGMP query message. (The default value is 100 tenths-of-seconds). Configured through the `ip multicast query-response-interval` command.
output definitions

<table>
<thead>
<tr>
<th>Last Member Query Interval (tenths of seconds)</th>
<th>Displays the time (in tenths of seconds) taken to reply to an IGMP query message sent in response to a leave group message. (The default value is 10 tenths-of-seconds.) Configured through the <code>ip multicast last-member-query-interval</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsolicited Report Interval (seconds)</td>
<td>Displays the time period (in seconds) to proxy any changed IGMP membership state. (The default value is 1 second). Configured through the <code>ip multicast unsolicited-report-interval</code> command.</td>
</tr>
<tr>
<td>Proxying</td>
<td>Whether IGMP proxying on the system is <strong>enabled</strong> or <strong>disabled</strong> (the default status). Configured through the <code>ip multicast proxying</code> command.</td>
</tr>
<tr>
<td>Spoofing</td>
<td>Whether IGMP spoofing on the system is <strong>enabled</strong> or <strong>disabled</strong> (the default status). Configured through the <code>ip multicast spoofing</code> command.</td>
</tr>
<tr>
<td>Zapping</td>
<td>Whether IGMP zapping on the system is <strong>enabled</strong> or <strong>disabled</strong> (the default status). Configured through the <code>ip multicast zapping</code> command.</td>
</tr>
<tr>
<td>Querier Forwarding</td>
<td>Whether IGMP querier forwarding on the system is <strong>enabled</strong> or <strong>disabled</strong> (the default status). Configured through the <code>ip multicast querier-forwarding</code> command.</td>
</tr>
<tr>
<td>Router Timeout (seconds)</td>
<td>Displays the IGMP router timeout in seconds. (The default value is 90 seconds.) Configured through the <code>ip multicast router-timeout</code> command.</td>
</tr>
<tr>
<td>Source Timeout (seconds)</td>
<td>Displays the IGMP source timeout in seconds. (The default value is 30 seconds.) Configured through the <code>ip multicast source-timeout</code> command.</td>
</tr>
<tr>
<td>Max-group</td>
<td>Displays the global maximum group limit that can be learned per VLAN instance. (The default value is 0, which means no limit is imposed). Configured through the <code>ip multicast max-group</code> command.</td>
</tr>
<tr>
<td>Max-group action</td>
<td>Displays the action taken when the maximum group limit has been exceeded (<strong>none</strong>, <strong>drop</strong> or <strong>replace</strong>). Configured through the <code>ip multicast max-group</code> command.</td>
</tr>
<tr>
<td>Helper-address</td>
<td>Displays the destination IP address of a relay host, where IGMP host reports and Leave messages are to be sent. (By default, no Helper-address is configured.) Configured through the <code>ip multicast helper-address</code> command. <em>This function is supported only in the VLAN domain; service domain is not supported.</em></td>
</tr>
<tr>
<td>Static Querier Address</td>
<td>The Static Source IP Address to be used when querying. (The default value of 0.0.0.0 indicates that this is not configured.) <em>This function is not supported.</em></td>
</tr>
<tr>
<td>Static Spoofing Address</td>
<td>The Static Source IP Address to be used when spoofing. (The default value of 0.0.0.0 indicates that this is not configured.) Configured through the <code>ip multicast spoofing static-source-ip</code> command.</td>
</tr>
<tr>
<td>Zero-based Query</td>
<td>Whether Zero-based Querying is <strong>disabled</strong> or <strong>enabled</strong> (the default status). Configured through the <code>ip multicast zero-based-query</code> command.</td>
</tr>
<tr>
<td>Forward Mode</td>
<td>Displays the current IPv4 Forwarding mode (<strong>asm</strong>, <strong>ssm</strong>, <strong>mac</strong>, or <strong>auto</strong>). Configured through the <code>ip multicast forward-mode</code> command.</td>
</tr>
</tbody>
</table>
### Release History

Release 7.1.1; command was introduced.
Release 8.3.1; display fields added.
Release 8.4.1; service parameter added.

### Related Commands

- **ip multicast admin-state** Enables or disables IP Multicast Switching and Routing on the specified VLAN, or on the system if no VLAN is specified.

### output definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Delay Interval</strong></td>
<td>Displays the amount of time (in milliseconds) between propagating IPMS state changes. (The default value is 0 milliseconds). Configured through the <code>ip multicast update-delay-interval</code> command.</td>
</tr>
<tr>
<td><strong>SSM Mapping</strong></td>
<td>Whether Source Specific Multicast (SSM) mapping is enabled or disabled (the default). When enabled, Any Source Multicast (ASM) group memberships are translated into SSM group memberships. Configured through the <code>ip multicast ssm-map</code> command. <em>This function is not supported.</em></td>
</tr>
<tr>
<td><strong>Fast Join</strong></td>
<td>Whether the IP Multicast Switching fast join functionality is enabled or disabled (the default). When enabled, forwarding entries are automatically created in hardware as soon as IGMP memberships are learned instead of waiting for the multicast traffic to reach the switch. Configured through the <code>ip multicast fast-join</code> command.</td>
</tr>
<tr>
<td><strong>Initial Packet Buffering</strong></td>
<td>The current state of Initial Packet Buffering, which can be enabled or disabled (the default status). Configured through the <code>ip multicast initial-packet-buffer admin-state</code> command. <em>This function is supported only in the VLAN domain; service domain is not supported.</em></td>
</tr>
<tr>
<td><strong>Max Flows</strong></td>
<td>The maximum number of IPv4 multicast flows buffered for initial packet. Configured through the <code>ip multicast initial-packet-buffer max-flow</code> command. <em>This function is supported only in the VLAN domain; service domain is not supported.</em></td>
</tr>
<tr>
<td><strong>Max Packets Per Flow</strong></td>
<td>The maximum number of initial packets buffered per IPv4 multicast flow. Configured through the <code>ip multicast initial-packet-buffer max-packet</code> command. <em>This function is supported only in the VLAN domain; service domain is not supported.</em></td>
</tr>
<tr>
<td><strong>Buffer Timeout</strong></td>
<td>The timeout value for the initial buffered IPv4 multicast packets. Configured through the <code>ip multicast initial-packet-buffer timeout</code> command. <em>This function is supported only in the VLAN domain; service domain is not supported.</em></td>
</tr>
<tr>
<td><strong>Min Delay</strong></td>
<td>The minimum delay to program the multicast replication index for IPv4 multicast flows buffered for initial packet. Configured through the <code>ip multicast initial-packet-buffer min-delay</code> command. <em>This function is supported only in the VLAN domain; service domain is not supported.</em></td>
</tr>
</tbody>
</table>
MIB Objects

alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigStatus
  alaIpmsConfigQuerying
  alaIpmsConfigProxying
  alaIpmsConfigSpoofing
  alaIpmsConfigZapping
  alaIpmsConfigQuerierForwarding
  alaIpmsConfigVersion
  alaIpmsConfigRobustness
  alaIpmsConfigQueryInterval
  alaIpmsConfigQueryResponseInterval
  alaIpmsConfigLastMemberQueryInterval
  alaIpmsConfigUnsolicitedReportInterval
  alaIpmsConfigResourceTimeout
  alaIpmsConfigSourceTimeout
  alaIpmsConfigMaxGroupLimit
  alaIpmsConfigMaxGroupExceedAction
  alaIpmsConfigZeroBasedQuery
  alaIpmsConfigStaticSsmMapping
  alaIpmsConfigFloodUnknown
  alaIpmsConfigUpdateDelayInterval
  alaIpmsConfigForwardMode
  alaIpmsConfigQueryingStaticSourceAddress
  alaIpmsConfigSpoofingStaticSourceAddress
  alaIpmsConfigInitialPacketBuffer
  alaIpmsConfigInitialPacketBufferMaxPacket
  alaIpmsConfigInitialPacketBufferMaxFlow
  alaIpmsConfigInitialPacketBufferTimeout
  alaIpmsConfigInitialPacketBufferMinDelay
  alaIpmsConfigHelperAddress
  alaIpmsConfigFastJoin
show ip multicast port

Displays the maximum group configuration applicable for the specified port or the specified Service Access Point (SAP) port. The current number of groups learned on a port, port/VLAN, SAP port, or SAP port/Shortest Path Bridging (SPB) service instance is also displayed.

`show ip multicast {port [chassis/slot/port | sap port [sap_id]}`

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port**
  - The slot and port number (3/1).

- **sap_id**
  - The SAP ID (chassis/slot/port:encapsulation). *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify a port number to display the configuration information for a specific switch port.
- Specify a SAP ID to display the configuration information for a specific SAP port.
- When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ip multicast static-querier service 10 sap port 1/1/23:10`, where 1/1/23:10 is the SAP ID).
- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port 1/1/23 with VLAN 10 encapsulation is 1/1/23:10. Any traffic received on port 1/1/23 that is tagged with VLAN 10 is mapped to the SPB service that is associated with the 1/1/23:10 SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.
**Examples**

`-> show ip multicast port`

**Legends:**
- Interface Max-group = Max-group limit on the interface
- Interface Action = Max-group action on the interface
- Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
- Interface-Instance Action = Active Max-group action on the Lan Interface instance

**Total 2 Lan Interface Instances**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/13</td>
<td>vlan 1036</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>1/1/52</td>
<td>vlan 1</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>

`-> show ip multicast port 1/1/52`

**Legends:**
- Interface Max-group = Max-group limit on the interface
- Interface Action = Max-group action on the interface
- Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
- Interface-Instance Action = Active Max-group action on the Lan Interface instance

**Total 2 Lan Interface Instances**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/52</td>
<td>vlan 1</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>

`-> show ip multicast sap port`

**Legends:**
- Interface Max-group = Max-group limit on the interface
- Interface Action = Max-group action on the interface
- Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
- Interface-Instance Action = Active Max-group action on the Lan Interface instance

**Total 2 Lan Interface Instances**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/5:100</td>
<td>service 20</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>sap:1/1/23:200</td>
<td>service 30</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>

`-> show ip multicast sap port 1/1/23:200`

**Legends:**
- Interface Max-group = Max-group limit on the interface
- Interface Action = Max-group action on the interface
- Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
- Interface-Instance Action = Active Max-group action on the Lan Interface instance

**Total 2 Lan Interface Instances**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/23:200</td>
<td>service 30</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Interface</th>
<th>The VLAN port or the SAP (chassis/slot/port:encapsulation) that serves as the virtual port for the SPB service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan/Service</td>
<td>The VLAN or SPB service ID associated with the IP multicast interface.</td>
</tr>
<tr>
<td>Current Groups</td>
<td>The current groups associated with the IP multicast interface.</td>
</tr>
<tr>
<td>Interface Max-group</td>
<td>The maximum group count allowed on the port or SAP port. This limit is applicable on the given port for all VLAN or service instances of the port.</td>
</tr>
<tr>
<td>Interface Action</td>
<td>The action to be taken when the group membership limit is exceeded (<strong>none</strong>, <strong>drop</strong>, or <strong>replace</strong>).</td>
</tr>
<tr>
<td>Interface-Instance Max-group</td>
<td>The maximum group limit learned per port for the given VLAN or per SAP port for the given SPB service. This limit is applied to each port that is a member of the given VLAN or each SAP port that is a member of the given service.</td>
</tr>
<tr>
<td>Interface-Instance Action</td>
<td>The action to be taken when the group membership limit is exceeded (<strong>none</strong>, <strong>drop</strong>, or <strong>replace</strong>).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.  
Release 8.4.1; sap port parameter added.

**Related Commands**

- **ip multicast port max-group**  
  Configures the maximum group limit learned per port.

- **ip multicast port max-group**  
  Configures the maximum group limit learned per port for the specified VLAN, SPB service, or on the system if no VLAN or SPB service is specified.

**MIB Objects**

- `alaIpmsIntfStatsConfigType`  
- `alaIpmsIntfStatsAddressType`  
- `alaIpmsIntfStatsValue`  
- `alaIpmsIntfStatsCurrentGroupCount`  
- `alaIpmsIntfStatsMaxGroupLimit`  
- `alaIpmsIntfStatsMaxGroupExceedAction`
show ip multicast forward

Displays the IP Multicast Switching and Routing forwarding table entries for the specified IP multicast group address or all the entries if no IP multicast group address is specified.

show ip multicast forward [ip_address] [vlan [vlan_id]-vlan_id2] [service [service_id]-service_id2]] [all-vrf]

Syntax Definitions

**ip_address**  
IP multicast group address.

**vlan [vlan_id]-vlan_id2**  
Display forwarding table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.

**service [service_id]-service_id2**  
Display forwarding table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.

**all-vrf**  
Display forwarding table entries for all of the VRF instances.

Defaults

By default, forwarding entries for all of the IP multicast groups are displayed for the current VRF instance.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **ip_address** parameter to display forwarding table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the forwarding table entries that exist in all of the VRF instances on the switch.
- Forwarding entries are derived by applying the state from the source table to the state in the group, neighbor, and querier tables.
- On an OmniSwitch 9900, this command is available only when IP Multicast Switching and Routing is enabled for the switch. To view the multicast forwarding database on an OmniSwitch 6465 or OmniSwitch 6560 or OmniSwitch 6570M, see the **show ip multicast bridge** and **show ip multicast bridge-forward** commands.
• Use the `ip multicast display-interface-names` command to enable displaying the associated IP interface name in the “Ingress Vlan/Service” and “Egress Vlan/Service” fields instead of the VLAN ID or service ID.

**Examples**

```
-> show ip multicast forward

Total 3 Forwards
Group Address  Host Address  Tunnel Address  Vlan/Service  Egress
---------------+--------------+--------------+------------+----------
225.0.1.0      21.20.20.2  0.0.0.0        vlan 20      vlan 20    1/1/2
225.0.1.0      21.20.20.2  0.0.0.0        service 10   service 10  sdp:32776
225.0.1.1      21.20.20.2  0.0.0.0        vlan 20      vlan 20    1/1/2
225.0.1.1      21.20.20.2  0.0.0.0        service 10   service 10  sdp:32776
225.0.1.2      21.20.20.2  0.0.0.0        vlan 20      vlan 21    1/1/2
225.0.1.2      21.20.20.2  0.0.0.0        service 10   service 10  sap:1/5:10
```

```
-> show ip multicast forward service

Total 3 Forwards
Group Address  Host Address  Tunnel Address  Vlan/Service  Egress
---------------+--------------+--------------+------------+----------
225.0.1.0      21.20.20.2  0.0.0.0        service 10   service 10  sdp:32776
225.0.1.1      21.20.20.2  0.0.0.0        service 10   service 10  sdp:32776
225.0.1.2      21.20.20.2  0.0.0.0        service 10   service 10  sap:1/5:10
```

```
-> show ip multicast forward vlan

Total 3 Forwards
Group Address  Host Address  Tunnel Address  Vlan/Service  Egress
---------------+--------------+--------------+------------+----------
225.0.1.0      21.20.20.2  0.0.0.0        vlan 20      vlan 20    1/1/2
225.0.1.1      21.20.20.2  0.0.0.0        vlan 20      vlan 20    1/1/2
225.0.1.2      21.20.20.2  0.0.0.0        vlan 20      vlan 21    1/1/2
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast forward vlan

Total 3 Forwards
Group Address  Host Address  Tunnel Address  Vlan/Service  Egress
---------------+--------------+--------------+------------+----------
225.0.1.0      21.20.20.2  0.0.0.0        VlanToLab    VlanToLab    1/1/2
225.0.1.1      21.20.20.2  0.0.0.0        VlanToLab    VlanToLab    1/1/2
225.0.1.2      21.20.20.2  0.0.0.0        VlanToLab    VlanToCore   1/1/2
```

**output definitions**

- **Group Address**: IP group address of the IP multicast forward.
- **Host Address**: IP host address of the IP multicast forward.
- **Tunnel Address**: IP source tunnel address of the IP multicast forward.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Vlan/Service</td>
<td>The ingress VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast forward. If the global display interface names option is enabled, then the ingress interface name associated with the IP multicast forward is displayed.</td>
</tr>
<tr>
<td>Egress Vlan/Service</td>
<td>The egress VLAN or SPB service ID associated with the IP multicast forward. If the global display interface names option is enabled, then the egress interface name associated with the IP multicast forward is displayed. The egress interface (port) will also be included in the forward entry with both output formats.</td>
</tr>
<tr>
<td>Interface</td>
<td>The VLAN port or SPB virtual port of the IP multicast forward.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.

**Related Commands**

- **ip multicast static-group** Creates a static IGMP group entry on a specified port on a specified VLAN.

**MIB Objects**

- `alaIpmsForwardTable`
  - `alaIpmsForwardConfigType`
  - `alaIpmsForwardAddressType`
  - `alaIpmsForwardValue`
  - `alaIpmsForwardGroupAddress`
  - `alaIpmsForwardHostAddress`
  - `alaIpmsForwardDestAddress`
  - `alaIpmsForwardOrigAddress`
  - `alaIpmsForwardType`
  - `alaIpmsForwardNextConfigType`
  - `alaIpmsForwardNextValue`
  - `alaIpmsForwardNextIfIndex`
  - `alaIpmsForwardNextType`
**show ip multicast neighbor**

Displays the IGMP neighbor table entries of IP Multicast Switching and Routing.

`show ip multicast neighbor [vlan [vlan_id]-[vlan_id2]] | service [service_id]-[service_id2]] | all-vrf`

### Syntax Definitions

**vlan [vlan_id]-[vlan_id2]**  
Display IGMP neighbor table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.

**service [service_id]-[service_id2]**  
Display IGMP neighbor table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

**all-vrf**  
Display IGMP neighbor table entries for all of the VRF instances.

### Defaults

By default, only the neighbor table entries specific to the current VRF instance are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `all-vrf` parameter option to display the neighbor table entries that exist in all of the VRF instances on the switch.

- Interfaces with neighbors receive all IPv4 multicast, including all IGMP traffic.

- Use the `ip multicast display-interface-names` command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

### Examples

```
-> show ip multicast neighbor

Total 12 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>170.0.0.2</td>
<td>vlan 2000 0/10</td>
<td>no</td>
<td>528</td>
<td>85</td>
</tr>
<tr>
<td>170.0.1.3</td>
<td>vlan 2001 0/1</td>
<td>no</td>
<td>502</td>
<td>66</td>
</tr>
<tr>
<td>170.0.59.45</td>
<td>vlan 2059 0/11</td>
<td>no</td>
<td>554</td>
<td>80</td>
</tr>
<tr>
<td>170.0.61.46</td>
<td>vlan 2061 0/12</td>
<td>no</td>
<td>553</td>
<td>79</td>
</tr>
</tbody>
</table>
```
show ip multicast neighbor

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>170.0.63.47</td>
<td>vlan 2063 0/13</td>
<td>no</td>
<td>553</td>
<td>66</td>
</tr>
<tr>
<td>170.0.65.48</td>
<td>vlan 2065 0/14</td>
<td>no</td>
<td>553</td>
<td>64</td>
</tr>
<tr>
<td>170.0.67.51</td>
<td>vlan 2067 1/5/31</td>
<td>no</td>
<td>475</td>
<td>86</td>
</tr>
<tr>
<td>170.0.69.52</td>
<td>vlan 2069 1/5/43</td>
<td>no</td>
<td>553</td>
<td>83</td>
</tr>
<tr>
<td>170.0.71.53</td>
<td>vlan 2071 1/6/31</td>
<td>no</td>
<td>552</td>
<td>61</td>
</tr>
<tr>
<td>170.0.73.54</td>
<td>vlan 2073 1/6/43</td>
<td>no</td>
<td>552</td>
<td>67</td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>service 20 SAP:1/5:10</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>service 20 SAP:1/5:20</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
</tbody>
</table>

-> show ip multicast neighbor service

Total 2 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>service 20 SAP:1/5:10</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>service 20 SAP:1/5:20</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
</tbody>
</table>

-> show ip multicast neighbor vlan

Total 10 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>170.0.0.2</td>
<td>vlan 2000 0/10</td>
<td>no</td>
<td>528</td>
<td>85</td>
</tr>
<tr>
<td>170.0.1.3</td>
<td>vlan 2001 0/1</td>
<td>no</td>
<td>502</td>
<td>66</td>
</tr>
<tr>
<td>170.0.59.45</td>
<td>vlan 2059 0/11</td>
<td>no</td>
<td>554</td>
<td>80</td>
</tr>
<tr>
<td>170.0.61.46</td>
<td>vlan 2061 0/12</td>
<td>no</td>
<td>553</td>
<td>79</td>
</tr>
<tr>
<td>170.0.63.47</td>
<td>vlan 2063 0/13</td>
<td>no</td>
<td>553</td>
<td>66</td>
</tr>
<tr>
<td>170.0.65.48</td>
<td>vlan 2065 0/14</td>
<td>no</td>
<td>553</td>
<td>64</td>
</tr>
<tr>
<td>170.0.67.51</td>
<td>vlan 2067 1/5/31</td>
<td>no</td>
<td>475</td>
<td>86</td>
</tr>
<tr>
<td>170.0.69.52</td>
<td>vlan 2069 1/5/43</td>
<td>no</td>
<td>553</td>
<td>83</td>
</tr>
<tr>
<td>170.0.71.53</td>
<td>vlan 2071 1/6/31</td>
<td>no</td>
<td>552</td>
<td>61</td>
</tr>
<tr>
<td>170.0.73.54</td>
<td>vlan 2073 1/6/43</td>
<td>no</td>
<td>552</td>
<td>67</td>
</tr>
</tbody>
</table>

-> show ip multicast neighbor vlan 2063

Total 1 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>170.0.63.47</td>
<td>vlan 2063 0/13</td>
<td>no</td>
<td>553</td>
<td>66</td>
</tr>
</tbody>
</table>

Sample output when the global display interface names option is enabled:

-> ip multicast display-interface-names

-> show ip multicast neighbor vlan 2063

Total 1 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>170.0.63.47</td>
<td>VlanToLab 0/13</td>
<td>no</td>
<td>553</td>
<td>66</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>The IP address of the IP multicast neighbor.</td>
</tr>
<tr>
<td>Vlan/Service</td>
<td>The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast neighbor. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast neighbor is displayed.</td>
</tr>
<tr>
<td>Interface</td>
<td>The VLAN port or the SPB virtual port of the IP multicast neighbor.</td>
</tr>
<tr>
<td>Static</td>
<td>Whether it is a static IP multicast neighbor or not.</td>
</tr>
<tr>
<td>Count</td>
<td>Displays the count of IP multicast neighbor.</td>
</tr>
<tr>
<td>Life</td>
<td>The life time of the IP multicast neighbor.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1; all-vrf parameter added.
Release 8.4.1; domain parameter added.
Release 8.4.1.R02; domain parameter deprecated.

**Related Commands**

**ip multicast static-neighbor**

Creates a static IGMP neighbor entry on a specified port on a specified VLAN.

**MIB Objects**

<table>
<thead>
<tr>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaIpmsNeighborTable</td>
</tr>
<tr>
<td>alaIpmsNeighborConfigType</td>
</tr>
<tr>
<td>alaIpmsNeighborAddressType</td>
</tr>
<tr>
<td>alaIpmsNeighborValue</td>
</tr>
<tr>
<td>alaIpmsNeighborIfIndex</td>
</tr>
<tr>
<td>alaIpmsNeighborHostAddress</td>
</tr>
<tr>
<td>alaIpmsNeighborCount</td>
</tr>
<tr>
<td>alaIpmsNeighborTimeout</td>
</tr>
<tr>
<td>alaIpmsNeighborUpTime</td>
</tr>
<tr>
<td>alaIpmsStaticNeighborTable</td>
</tr>
<tr>
<td>alaIpmsStaticNeighborConfigType</td>
</tr>
<tr>
<td>alaIpmsStaticNeighborAddressType</td>
</tr>
<tr>
<td>alaIpmsStaticNeighborValue</td>
</tr>
<tr>
<td>alaIpmsStaticNeighborIfIndex</td>
</tr>
<tr>
<td>alaIpmsStaticNeighborRowStatus</td>
</tr>
</tbody>
</table>
**show ip multicast querier**

Displays the IGMP querier table entries of IP Multicast Switching and Routing.

```
show ip multicast querier [vlan [vlan_id]-vlan_id2] | service [service_id]-service_id2]] [all-vrf]
```

### Syntax Definitions

- **vlan [vlan_id]-vlan_id2**: Display IGMP querier table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- **service [service_id]-service_id2**: Display IGMP querier table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **all-vrf**: Display IGMP querier table entries for all of the VRF instances.

### Defaults

By default, only IGMP querier entries specific to the current VRF instance are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **all-vrf** parameter option to display the IGMP querier table entries that exist in all of the VRF instances on the switch.
- Interfaces with queriers receive all IGMP traffic, and if querier forwarding is enabled, these interfaces will also receive all IPv4 multicast traffic.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

### Examples

```
-> show ip multicast querier

Total 10 Queriers

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.1.254.96</td>
<td>vlan 1001 0/1</td>
<td>no</td>
<td>3</td>
<td>213</td>
</tr>
<tr>
<td>172.2.254.96</td>
<td>vlan 1002 0/1</td>
<td>no</td>
<td>4</td>
<td>213</td>
</tr>
<tr>
<td>172.3.254.96</td>
<td>vlan 1003 0/1</td>
<td>no</td>
<td>4</td>
<td>214</td>
</tr>
</tbody>
</table>
```
show ip multicast querier

```
172.4.254.96  vlan 1004  0/1  no  4   213
172.5.254.96  vlan 1005  0/1  no  4   213
172.6.254.96  vlan 1006  0/1  no  4   213
172.7.254.96  vlan 1007  0/1  no  4   213
172.8.254.96  vlan 1008  0/1  no  4   213
225.0.1.0     service 10 SAP:1/5:10 no    5520  172
225.0.1.0     service 10 SAP:1/5:20 no    5520  172
```

-> show ip multicast querier service

Total 2 Queriers

```
Host Address  Vlan/Service Interface  Static  Count  Life
---------------+----------------+-------+------+-----+
225.0.1.0     service 10 SAP:1/5:10 no    5520  172
225.0.1.0     service 10 SAP:1/5:20 no    5520  172
```

-> show ip multicast querier vlan

Total 8 Queriers

```
Host Address  Vlan/Service Interface  Static  Count  Life
---------------+----------------+-------+------+-----+
172.1.254.96  vlan 1001  0/1  no  3   213
172.2.254.96  vlan 1002  0/1  no  4   213
172.3.254.96  vlan 1003  0/1  no  4   214
172.4.254.96  vlan 1004  0/1  no  4   213
172.5.254.96  vlan 1005  0/1  no  4   213
172.6.254.96  vlan 1006  0/1  no  4   213
172.7.254.96  vlan 1007  0/1  no  4   213
172.8.254.96  vlan 1008  0/1  no  4   213
```

Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
```

```
-> show ip multicast querier vlan
```

Total 8 Queriers

```
Host Address  Vlan/Service Interface  Static  Count  Life
---------------+----------------+-------+------+-----+
172.1.254.96  VlanToLab    0/1  no  3   213
172.2.254.96  VlanToLab    0/1  no  4   213
172.3.254.96  VlanToLab    0/1  no  4   214
172.4.254.96  VlanToLab    0/1  no  4   213
172.5.254.96  VlanToLab    0/1  no  4   213
172.6.254.96  VlanToLab    0/1  no  4   213
172.7.254.96  VlanToLab    0/1  no  4   213
172.8.254.96  VlanToLab    0/1  no  4   213
```
output definitions

<table>
<thead>
<tr>
<th>Host Address</th>
<th>The IP address of the IP multicast querier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan/Service</td>
<td>The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast querier. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast querier is displayed.</td>
</tr>
<tr>
<td>Interface</td>
<td>The VLAN port or the SPB virtual port of the IP multicast querier.</td>
</tr>
<tr>
<td>Static</td>
<td>Whether it is a static multicast neighbor or not.</td>
</tr>
<tr>
<td>Count</td>
<td>Displays the count of the IP multicast querier.</td>
</tr>
<tr>
<td>Life</td>
<td>The life time of the IP multicast querier.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; all-vrf parameter added.
Release 8.4.1; domain parameter added.
Release 8.4.1.R02; domain parameter deprecated.

Related Commands

ip multicast static-querier  Creates a static IGMP querier entry on a specified port on a specified VLAN.

MIB Objects

alaIpmsQuerierTable
alaIpmsQuerierConfigType
alaIpmsQuerierAddressType
alaIpmsQuerierValue
alaIpmsQuerierIfIndex
alaIpmsQuerierHostAddress
alaIpmsQuerierCount
alaIpmsQuerierTimeout
alaIpmsQuerierUpTime
alaIpmsStaticQuerierTable
alaIpmsStaticQuerierConfigType
alaIpmsStaticQuerierAddressType
alaIpmsStaticQuerierValue
alaIpmsStaticQuerierIfIndex
alaIpmsStaticQuerierRowStatus
**show ip multicast group**

Displays the IGMP group membership table entries of IP Multicast Switching and Routing for the specified IP multicast group address or all entries if no IP multicast group address is specified.

`show ip multicast group [ip_address] [vlan [vlan_id]-vlan_id2] | service [service_id]-service_id2] [all-vrf]`

### Syntax Definitions

- **ip_address**: IP multicast group address.
- **vlan [vlan_id]-vlan_id2**: Display group membership entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- **service [service_id]-service_id2**: Display group membership entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- **all-vrf**: Display group membership entries for all of the VRF instances.

### Defaults

By default, all IP multicast groups are displayed for the current VRF instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **ip_address** parameter to display entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the IGMP group membership table entries that exist in all of the VRF instances on the switch.
- Use the **ip multicast display-interface-names** command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

### Examples

```
-> show ip multicast group

Total 8 Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
<td>1/1/19</td>
<td>exclude</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
</tbody>
</table>
```
IP Multicast Switching Commands

show ip multicast group

Total 1 Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
<td>1/1/19</td>
<td>exclude yes</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>service 20</td>
<td>SAP:1/5:10</td>
<td>no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>service 20</td>
<td>SAP:1/5:20</td>
<td>no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>service 20</td>
<td>sdp:32776</td>
<td>no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
</tbody>
</table>

Total 3 Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>service 20</td>
<td>SAP:1/5:10</td>
<td>no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>service 20</td>
<td>SAP:1/5:20</td>
<td>no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>service 20</td>
<td>sdp:32776</td>
<td>no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
</tbody>
</table>

Total 5 Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
<td>1/1/19</td>
<td>exclude yes</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
<td>1/1/19</td>
<td>exclude no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
<td>1/1/19</td>
<td>exclude no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.3</td>
<td>0.0.0.0</td>
<td>vlan 100</td>
<td>1/1/1</td>
<td>exclude yes</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>225.0.1.4</td>
<td>0.0.0.0</td>
<td>vlan 101</td>
<td>1/1/1</td>
<td>exclude yes</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

Sample output when the global display interface names option is enabled:

-> show ip multicast display-interface-names

-> show ip multicast group vlan

Total 5 Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
<td>1/1/19</td>
<td>exclude no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
<td>1/1/19</td>
<td>exclude no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
<td>1/1/19</td>
<td>exclude no</td>
<td>5520</td>
<td>172</td>
<td></td>
</tr>
<tr>
<td>225.0.1.3</td>
<td>0.0.0.0</td>
<td>VlanToCore</td>
<td>1/1/1</td>
<td>exclude yes</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>225.0.1.4</td>
<td>0.0.0.0</td>
<td>VlanToDist</td>
<td>1/1/1</td>
<td>exclude yes</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
</table>

- **Group Address**: IP address of the IP multicast group.
- **Source Address**: IP address of the IP multicast source.
output definitions

| Vlan/Service | The VLAN or Shortest Path Bridging (SPB) service ID associated with the IPv4 multicast group. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast group is displayed. |
| Interface | The VLAN port or the SPB virtual port on which the group membership was learned. |
| Mode | IGMP source filter mode. |
| Static | Whether it is a static multicast group or not. |
| Count | Number of IGMP membership requests made. |
| Life | Life time of the IGMP group membership. |

Release History

Release 7.1.1; command was introduced
Release 8.3.1; all-vrf parameter added.
Release 8.4.1; domain parameter added.
Release 8.4.1.R02; domain parameter deprecated.

Related Commands.

**ip multicast static-group**

Creates a static IGMP group entry on a specified port for the specified VLAN or on the specified SPB virtual port for the specified SPB service.

MIB Objects

alaIpmsMemberTable

- alaIpmsMemberConfigType
- alaIpmsMemberAddressType
- alaIpmsMemberValue
- alaIpmsMemberIfIndex
- alaIpmsMemberGroupAddress
- alaIpmsMemberSourceAddress
- alaIpmsMemberMode
- alaIpmsMemberCount
- alaIpmsMemberTimeout

alaIpmsStaticMemberTable

- alaIpmsStaticMemberConfigType
- alaIpmsStaticMemberConfigAddressType
- alaIpmsStaticMemberValue
- alaIpmsStaticMemberIfIndex
- alaIpmsStaticMemberGroupAddress
- alaIpmsStaticMemberRowStatus
show ip multicast source

Displays the IP Multicast Switching and Routing source table entries matching the specified IP multicast group address or all entries if no IP multicast group address is specified.

`show ip multicast source [ip_address] [vlan [vlan_id]-vlan_id2] [service [service_id]-service_id2] [all-vrf]`

**Syntax Definitions**

`ip_address` | IP multicast group address.
---|---
`vlan [vlan_id]-vlan_id2` | Displays source table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
`service [service_id]-service_id2` | Displays source table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
`all-vrf` | Display source table entries for all of the VRF instances.

**Defaults**

By default, all source table entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `ip_address` parameter to display source entries for a specific multicast group.

- In the service domain, only the first flow that is used to learn the source is displayed. Use the `extended` parameter to display other possible multicast IP addresses matching the same multicast MAC address. In this case, an asterisk (*) in the “Host Address” field represents the other multicast IP addresses.

- Use the `all-vrf` parameter option to display the source table entries that exist in all of the VRF instances on the switch.

- On an OmniSwitch 9900, this command is available only when IP Multicast Switching and Routing is enabled for the switch. To view the multicast forwarding database on an OmniSwitch 6465 or OmniSwitch 6560 or OmniSwitch 6570M, see the `show ip multicast bridge` and `show ip multicast bridge-forward` commands.

- Use the `ip multicast display-interface-names` command to enable displaying the associated IP interface name in the “Ingress Vlan/Service” field instead of the VLAN ID or service ID.
**Examples**

-> show ip multicast source

Total 10 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.0</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>service 20</td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>service 20</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>service 20</td>
</tr>
<tr>
<td>225.0.1.3</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.3</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>service 20</td>
</tr>
<tr>
<td>225.0.1.4</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.4</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>service 20</td>
</tr>
</tbody>
</table>

-> show ip multicast source 225.0.1.2

Total 2 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>service 20</td>
</tr>
</tbody>
</table>

-> show ip multicast source service

Total 5 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>20</td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>20</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>20</td>
</tr>
<tr>
<td>225.0.1.3</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>20</td>
</tr>
<tr>
<td>225.0.1.4</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>20</td>
</tr>
</tbody>
</table>

-> show ip multicast source vlan

Total 5 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.3</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
<tr>
<td>225.0.1.4</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>vlan 21</td>
</tr>
</tbody>
</table>
Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast source vlan
```

Total 5 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source Tunnel Address</th>
<th>Ingress Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>225.0.1.3</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>225.0.1.4</td>
<td>21.20.20.2</td>
<td>0.0.0.0</td>
<td>VlanToLab</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source Tunnel Address</th>
<th>Ingress Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP group address of the IP multicast source.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP host address of the IP multicast source.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP destination tunnel address of the IP multicast source.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The ingress VLAN or Shortest Path Bridging (SPB) service ID number associated with the IP multicast source. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast source is displayed.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1; all-vrf parameter added.
Release 8.4.1; domain parameter added.
Release 8.4.1.R02; domain parameter deprecated.

**Related Commands**

**show ip multicast tunnel**
Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

**MIB Objects**

alaIpmsSourceTable
alaIpmsSourceConfigType
alaIpmsSourceAddressType
alaIpmsSourceValue
alaIpmsSourceGroupAddress
alaIpmsSourceHostAddress
alaIpmsSourceDestAddress
alaIpmsSourceOrigAddress
alaIpmsSourceType
alaIpmsSourceUpTime
**show ip multicast tunnel**

Displays the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

```
show ip multicast tunnel [ip_address] [vlan [vlan_id]-vlan_id2] [service [service_id]-service_id2] [all-vrf]
```

**Syntax Definitions**

- `ip_address` (IP multicast group address.)
- `vlan [vlan_id]-vlan_id2` (Displays tunneling table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.)
- `service [service_id]-service_id2` (Displays tunneling table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*)
- `all-vrf` (Display the tunneling table entries for all of the VRF instances.)

**Defaults**

By default, all tunnel entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `ip_address` parameter to display the tunnel entries for a specific multicast group.
- Use the `all-vrf` parameter option to display the IP multicast tunnel entries that exist in all of the VRF instances on the switch.
- Use the `ip multicast display-interface-names` command to enable displaying the associated IP interface name in the “Ingress Vlan/Service” field instead of the VLAN ID or service ID.

**Examples**

```
-> show ip multicast tunnel

Total 3 Tunnels

<table>
<thead>
<tr>
<th>Destination</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Host Address</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
```
Sample output when the global display interface names option is enabled:

```
-> ip multicast display-interface-names
-> show ip multicast tunnel
```

### Total 3 Tunnels

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Ingress Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>21.20.20.2</td>
<td>10.10.10.51</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>21.20.20.2</td>
<td>10.10.10.51</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>225.0.1.2</td>
<td>21.20.20.2</td>
<td>10.10.10.51</td>
<td>VlanToLab</td>
</tr>
</tbody>
</table>

### Output Definitions

- **Group Address**: IP group address of the IP multicast tunnel.
- **Host Address**: IP host address of the IP multicast tunnel.
- **Destination Tunnel Address**: IP source tunnel address of the IP multicast tunnel.
- **Ingress Vlan/Service**: VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast tunnel. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast tunnel is displayed.

### Release History

- **Release 7.1.1**: command was introduced.
- **Release 8.3.1**: `all-vrf` parameter added.
- **Release 8.4.1.R02**: `vlan` and `service` parameters added.

### Related Commands

- **`show ip multicast source`**: Displays the IP Multicast Switching and Routing source table entries matching the specified IP multicast group address or all entries if no IP multicast group address is specified

### MIB Objects

```
alaIpmsTunnelTable
  alaIpmsTunnelConfigType
  alaIpmsTunnelAddressType
  alaIpmsTunnelValue
  alaIpmsTunnelGroupAddress
  alaIpmsTunnelHostAddress
  alaIpmsTunnelDestAddress
  alaIpmsTunnelOrigAddress
  alaIpmsTunnelType
  alaIpmsTunnelNextDestAddress
  alaIpmsTunnelNextType
```
show ip multicast host-list

Displays the IP multicast host address list configuration for the switch.

show ip multicast host-list [host_list_name]

Syntax Definitions

host_list_name
The name of an existing IP multicast host list.

Defaults
By default, all host lists configured on the switch are displayed.

Platforms Supported
Not supported in this release.

Usage Guidelines
Use the host_list_name parameter to display information for a specific host list.

Examples

-> show ip multicast host-list

Total 2 Lists

<table>
<thead>
<tr>
<th>Host List Name</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-map1</td>
<td>10.2.2.1</td>
</tr>
<tr>
<td></td>
<td>10.2.2.3</td>
</tr>
<tr>
<td></td>
<td>10.2.2.4</td>
</tr>
<tr>
<td></td>
<td>10.2.2.5</td>
</tr>
<tr>
<td>ssm-map1</td>
<td>20.2.2.1</td>
</tr>
<tr>
<td></td>
<td>20.2.2.2</td>
</tr>
<tr>
<td></td>
<td>20.2.2.3</td>
</tr>
</tbody>
</table>

-> show ip multicast host-list ssm-map1

<table>
<thead>
<tr>
<th>Host List Name</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssm-map1</td>
<td>20.2.2.1</td>
</tr>
<tr>
<td></td>
<td>20.2.2.2</td>
</tr>
<tr>
<td></td>
<td>20.2.2.3</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1.R02; command introduced.
Related Commands

**ip multicast host-list**

Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

MIB Objects

- `alaIpmsHostListTable`
- `alaIpmsHostListName`
- `alaIpmsHostListAddressType`
- `alaIpmsHostListAddress`
show ip multicast ssm-map

Displays the Source Specific Multicast (SSM) mapping configuration for the switch.

show ip multicast ssm-map [vlan vlan_id]

Syntax Definitions

vlan_id VLAN for which to display the configuration.

Defaults
By default, all SSM mappings configured on the switch are displayed.

Platforms Supported
Not supported in this release.

Usage Guidelines
Specify a VLAN ID to display the configuration information for a specific VLAN.

Examples

-> show ip multicast ssm-map
Type    Id    Group Address/Prefix  Source List Name
-------+-----+---------------------+--------------------------------
global  0     225.20.1.1/32         h-list1
vlan    200   229.30.1.1/32         h-list2

-> show ip multicast ssm-map vlan 200
Type    Id    Group Address/Prefix  Source List Name
-------+-----+---------------------+--------------------------------
vlan    200   229.30.1.1/32         h-list2

Release History
Release 8.3.1.R02; command introduced.

Related Commands
ip multicast ssm-map Configures a list of host IP addresses.

MIB Objects
alaIpmsSsmMapTable
  alaIpmsSsmMapConfigType
  alaIpmsSsmMapConfigAddressType
  alaIpmsSsmMapConfigValue
  alaIpmsSsmMapGroupId
  alaIpmsSsmMapGroupPrefixLength
  alaIpmsSsmMapSourceListName
**show ip multicast bridge**

Displays the IP multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IP multicast group address, MAC address, or all entries if no additional parameters are specified.

`show ip multicast bridge [vlan [vlan_id|-vlan_id2] | service [service_id|-service_id2] | ip_address | mac_address] [all-vrf]`

**Syntax Definitions**

- **vlan [vlan_id|-vlan_id2]**: Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- **service [service_id|-service_id2]**: Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **ip_address**: IP multicast group address.
- **mac_address**: Group MAC address.
- **all-vrf**: Display bridge table entries for all of the VRF instances.

**Defaults**

By default, all bridge table entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use one of the optional parameters *(vlan_id, service_id, ip_address, mac_address)* to display bridge table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC).
  - The “Host Address” field will display zero (MAC) or the IP host address for the bridge entry (ASM or SSM).
Examples

-> show ip multicast bridge

Total 2 Bridge Entries

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>Type</th>
<th>Group Address</th>
<th>Host Address</th>
<th>Action</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 1</td>
<td>asm</td>
<td>224.1.2.3</td>
<td></td>
<td>forwarding</td>
<td>00d:00h:00m</td>
</tr>
<tr>
<td>vlan 10</td>
<td>mac</td>
<td>01-00-5e-09-08-07</td>
<td></td>
<td>forwarding</td>
<td>00d:00h:00m</td>
</tr>
</tbody>
</table>

-> show ip multicast bridge vlan 10

Total 1 Bridge Entries

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>Type</th>
<th>Group Address</th>
<th>Host Address</th>
<th>Action</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 10</td>
<td>mac</td>
<td>01-00-5e-09-08-07</td>
<td></td>
<td>forwarding</td>
<td>00d:00h:00m</td>
</tr>
</tbody>
</table>

output definitions

Vlan/Service The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.

Type The bridge entry type (asm, ssm, mac). Configured through the ip multicast forward-mode command.

Group Address If the bridge entry type is ASM or SSM, this field displays the destination IP group address; if the bridge entry type is MAC, this field displays the destination MAC address.

Host Address The source IP host address (only applies to SSM bridge entries, otherwise this field is blank).

Action The current action taken for the bridge entry (forwarding or filtering).

UpTime The amount of time that has elapsed since the bridge entry was created.

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02: service parameter added.

Related Commands

show ip multicast bridge-forward Displays the forwarding state of the IP multicast bridge table entries.

MIB Objects

alaIpmsBridgeTable
  alaIpmsBridgeConfigType
  alaIpmsBridgeAddressType
  alaIpmsBridgeValue
  alaIpmsBridgeType
  alaIpmsBridgeGroupAddress
  alaIpmsBridgeHostAddress
  alaIpmsBridgeUpTime
  alaIpmsBridgeAction
**show ip multicast bridge-forward**

Displays the forwarding state of the IP multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IP multicast group address, MAC address, or all entries if no additional parameters are specified.

```
show ip multicast bridge-forward [vlan [vlan_id]-vlan_id2] | service [service_id]-service_id2] | ip_address | mac_address] [all-vrf]
```

**Syntax Definitions**

- **vlan [vlan_id]-vlan_id2**
  - Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.

- **service [service_id]-service_id2**
  - Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

- **ip_address**
  - IP multicast group address.

- **mac_address**
  - Group MAC address.

- **all-vrf**
  - Display bridge table entries for all of the VRF instances.

**Defaults**

By default, all bridge table entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use one of the optional parameters (vlan_id, service_id, ip_address, mac_address) to display forwarding information for a specific multicast group.

- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.

- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC). In the examples for this command, the forwarding mode is changed to MAC to show how the “Group Address” field changes.
  - The “Host Address” field will display zero (MAC) or the IP host address for the bridge entry (ASM or SSM).
**Examples**

-> show ip multicast bridge-forward

Total 2 Bridge Entries

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>Type</th>
<th>Group Address</th>
<th>Host Address</th>
<th>Next Interface</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 1</td>
<td>asm</td>
<td>224.1.2.3</td>
<td></td>
<td>1/4/12</td>
<td>00h:00m:01s</td>
</tr>
<tr>
<td>vlan 10</td>
<td>mac</td>
<td>01-00-5e-09-08-07</td>
<td></td>
<td>1/4/12</td>
<td>00h:00m:05s</td>
</tr>
</tbody>
</table>

-> show ip multicast bridge-forward vlan 10

Total 1 Bridge Entries

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>Type</th>
<th>Group Address</th>
<th>Host Address</th>
<th>Next Interface</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 10</td>
<td>mac</td>
<td>01-00-5e-09-08-07</td>
<td></td>
<td>1/4/12</td>
<td>00h:00m:05s</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>The bridge entry type (asm, ssm, mac). Configured through the ip multicast forward-mode command.</td>
</tr>
<tr>
<td>Group Address</td>
<td>If the bridge entry type is ASM or SSM, this field displays the destination IP group address; if the bridge entry type is MAC, this field displays the destination MAC address.</td>
</tr>
<tr>
<td>Host Address</td>
<td>The source IP host address (only applies to SSM bridge entries, otherwise this field is blank).</td>
</tr>
<tr>
<td>Next Interface</td>
<td>The destination interface for the bridge forwarding entry.</td>
</tr>
<tr>
<td>UpTime</td>
<td>The amount of time that has elapsed since the bridge forward entry was created.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.3.1; command introduced.
Release 8.4.1.R02: service parameter added.

**Related Commands**

*show ip multicast bridge* Displays the IP multicast bridge table entries.

**MIB Objects**

alaIpmsBridgeForwardTable
  alaIpmsBridgeForwardConfigType,
  alaIpmsBridgeForwardAddressType,
  alaIpmsBridgeForwardValue,
  alaIpmsBridgeForwardType,
  alaIpmsBridgeForwardGroupAddress,
  alaIpmsBridgeForwardHostAddress,
  alaIpmsBridgeForwardNextIfIndex,
  alaIpmsBridgeForwardNextSubValue
  alaIpmsBridgeForwardUpTime
**show ip multicast bidir-forward**

Displays the IP multicast Bidirectional Protocol Independent Multicast (BIDIR-PIM) forwarding table entries for the specified IP multicast group address or all the entries if no IP multicast group address is specified.

```
show ip multicast bidir-forward [ip_address] [all-vrf]
```

### Syntax Definitions

- **ip_address**
  - IP multicast group address.

- **all-vrf**
  - Display forwarding table entries for all of the virtual routing and forwarding (VRF) instances.

### Defaults

By default, BIDIR-PIM forwarding entries for all of the IP multicast groups are displayed for the current VRF instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **ip_address** parameter to display BIDIR-PIM forwarding table entries for a specific multicast group.
- Use the **all-vrf** parameter option to display the BIDIR-PIM forwarding table entries that exist in all of the VRF instances on the switch.

### Examples

```
-> vrf vrf-1 show ip multicast bidir-forward
VRF:vrf-1  Total 2 Forwards

Egress
Group Address  Vlan/Service  Interface
---------------+-------------+-----------
225.0.1.0      vlan 30     1/2/1
  vlan 30     1/2/2
```
show ip multicast bidir-forward all-vrf

VRF:default  Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>vlan 20</td>
<td>1/1/1</td>
</tr>
<tr>
<td></td>
<td>vlan 20</td>
<td>1/1/2</td>
</tr>
<tr>
<td>225.0.1.1</td>
<td>vlan 21</td>
<td>1/1/2</td>
</tr>
</tbody>
</table>

VRF:vrf-1  Total 2 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.1.0</td>
<td>vlan 30</td>
<td>1/2/1</td>
</tr>
<tr>
<td></td>
<td>vlan 30</td>
<td>1/2/2</td>
</tr>
</tbody>
</table>

output definitions

- **VRF**: The VRF instance for the BIDIR route.
- **Group Address**: IP group address for the BIDIR route.
- **Egress VLAN/Service**: The destination VLAN or Shortest Path Bridging (SPB) service for the BIDIR route.
- **Interface**: Destination VLAN port or SPB virtual port for the BIDIR route.

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

- **show ip multicast bridge-forward**: Displays the forwarding state of the IP multicast bridge table entries.

MIB Objects

- alaIpmsForwardTable
  - alaIpmsBidirForwardAddressType
  - alaIpmsBidirForwardGroupAddress
  - alaIpmsBidirForwardType
  - alaIpmsBidirForwardValue
  - alaIpmsBidirForwardIfindex
  - alaIpmsBidirForwardSubValue
show ip multicast profile

Displays a list of available IPMS configuration profiles or the parameter settings for a specific profile.

show ip multicast profile [profile_name]

Syntax Definitions

profile_name
The name of an existing IPMS profile.

Defaults
By default, a list of available profiles is displayed.

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
The specified profile name must already exist in the switch configuration.

Examples

-> show ip multicast profile

Total 2 Profiles

Profile Name
---------------------
default
IGMPv3 with Zapping

-> show ip multicast profile "IGMPv3 with Zapping"

Status = enabled,
Flood Unknown = none,
Version = 3,
Robustness = 0,
Querying = none,
Query Interval (seconds) = 0,
Query Response Interval (tenths of seconds) = 0,
Last Member Query Interval (tenths of seconds) = 0,
Unsolicited Report Interval (seconds) = 0,
Proxying = enabled,
Spoofing = none,
Zapping = enabled,
Querier Forwarding = none,
Router Timeout (seconds) = 0,
Source Timeout (seconds) = 0,
Max-group = 0,
Max-group action = none,
Helper-address = 0.0.0.0,
Static Querier Address = 0.0.0.0,
Static Spoof Address = 0.0.0.0,
Zero-based Query = none,
Forward Mode = none,
Update Delay Interval (milliseconds) = 0,
SSM Mapping = none,
Fast Join = none,
Initial Packet Buffering = none,
  Max Flows = 0,
  Max Packets Per Flow = 0,
  Buffer Timeout (seconds) = 0,
  Min Delay (milliseconds) = 0

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

**ip multicast profile**
Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.

**ip multicast apply-profile**
Applies the specified IPMS profile to the specified IPMS instance.

**show ip multicast**
Displays the profile assignment for the IPMS instance.

MIB Objects

alaIpmsProfileTable
  alaIpmsProfileAddressType
  alaIpmsProfileName
  alaIpmsProfileIndex
  alaIpmsProfileRowStatus
alaIpmsConfigTable
  alaIpmsConfigType
  alaIpmsConfigAddressType
  alaIpmsConfigValue
  alaIpmsConfigProfileName
show ipv6 multicast

Displays the IPv6 Multicast Switching and Routing status and the general configuration parameters on the specified VLAN, Shortest Path Bridging (SPB) service, or on the system if no VLAN or SPB service is specified.

show ipv6 multicast [vlan vlan_id | service service_id]

Syntax Definitions

- **vlan_id**: VLAN for which to display the configuration.
- **service_id**: SPB service ID number (1–32767). *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

Defaults

By default, the status and general configuration parameters for the system are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specify a VLAN ID to display the configuration information for a specific VLAN.
- Specify an SPB service ID to display the configuration information for a specific SPB service.

Examples

```
-> show ipv6 multicast
Profile = default,
Status = disabled,
Flood Unknown = disabled,
Version = 1,
Robustness = 2,
Querying = disabled,
Query Interval (seconds) = 125,
Query Response Interval (milliseconds) = 10000,
Last Member Query Interval (milliseconds) = 1000,
Unsolicited Report Interval (seconds) = 1,
Proxying = disabled,
Spoofing = disabled,
Zapping = disabled,
```
Querier Forwarding = disabled,
Router Timeout (seconds) = 90,
Source Timeout (seconds) = 30,
Max-group = 0,
Max-group action = none,
Helper-address = ::,
Static Querier Address = ::,
Static Spoofed Address = ::,
Zero-based Query = enabled,
Forward Mode = auto,
Update Delay Interval (milliseconds) = 0,
SSM Mapping = disabled,
Fast Join
Initial Packet Buffering
  Max Flows = 32,
  Max Packets Per Flow = 32,
  Buffer Timeout (seconds) = 10,
  Min Delay (milliseconds) = 0

-> show ipv6 multicast vlan 200

Profile = default,
Status = disabled,
Flood Unknown = disabled,
Version = 1,
Robustness = 2,
Querying = disabled,
Query Interval (seconds) = 125,
Query Response Interval (milliseconds) = 10000,
Last Member Query Interval (milliseconds) = 1000,
Unsolicited Report Interval (seconds) = 1,
Proxying = disabled,
Spoofing = disabled,
Zapping = disabled,
Querier Forwarding = disabled,
Router Timeout (seconds) = 90,
Source Timeout (seconds) = 30,
Max-group = 0,
Max-group action = none,
Helper-address = ::,
Static Querier Address = ::,
Static Spoofed Address = ::,
Zero-based Query = disabled,
Forward Mode = auto,
Update Delay Interval (milliseconds) = 0,
SSM Mapping = disabled,
Fast Join
Initial Packet Buffering
  Max Flows = 32,
  Max Packets Per Flow = 32,
  Buffer Timeout (seconds) = 10,
  Min Delay (milliseconds) = 0

-> show ipv6 multicast service 20

Profile = default,
Status = disabled,
Flood Unknown = disabled,
Version = 1,
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Robustness</td>
<td>2</td>
</tr>
<tr>
<td>Querying</td>
<td>disabled</td>
</tr>
<tr>
<td>Query Interval (seconds)</td>
<td>125</td>
</tr>
<tr>
<td>Query Response Interval (milliseconds)</td>
<td>10000</td>
</tr>
<tr>
<td>Last Member Query Interval (milliseconds)</td>
<td>1000</td>
</tr>
<tr>
<td>Unsolicited Report Interval (seconds)</td>
<td>1</td>
</tr>
<tr>
<td>Proxying</td>
<td>disabled</td>
</tr>
<tr>
<td>Spoofing</td>
<td>disabled</td>
</tr>
<tr>
<td>Zapping</td>
<td>disabled</td>
</tr>
<tr>
<td>Querier Forwarding</td>
<td>disabled</td>
</tr>
<tr>
<td>Router Timeout (seconds)</td>
<td>0</td>
</tr>
<tr>
<td>Source Timeout (seconds)</td>
<td>300</td>
</tr>
<tr>
<td>Max-group</td>
<td>0</td>
</tr>
<tr>
<td>Max-group action</td>
<td>none</td>
</tr>
<tr>
<td>Helper-address</td>
<td>::</td>
</tr>
<tr>
<td>Static Querier Address</td>
<td>::</td>
</tr>
<tr>
<td>Static Spoof Address</td>
<td>::</td>
</tr>
<tr>
<td>Zero-based Query</td>
<td>disabled</td>
</tr>
<tr>
<td>Forward Mode</td>
<td>mac</td>
</tr>
<tr>
<td>Update Delay Interval (milliseconds)</td>
<td>0</td>
</tr>
<tr>
<td>SSM Mapping</td>
<td>disabled</td>
</tr>
<tr>
<td>Fast Join</td>
<td>disabled</td>
</tr>
<tr>
<td>Initial Packet Buffering</td>
<td>disabled</td>
</tr>
<tr>
<td>Max Flows</td>
<td>32</td>
</tr>
<tr>
<td>Max Packets Per Flow</td>
<td>32</td>
</tr>
<tr>
<td>Buffer Timeout (seconds)</td>
<td>10</td>
</tr>
<tr>
<td>Min Delay (milliseconds)</td>
<td>0</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th><strong>Profile</strong></th>
<th>The name of a predefined IPMS configuration profile that is assigned to this instance. Configured through the <code>ipv6 multicast profile</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Whether the IPv6 Multicast Switching and Routing is <strong>Enabled</strong> or <strong>Disabled</strong> (the default status). Configured through the <code>ipv6 multicast admin-state</code> command.</td>
</tr>
<tr>
<td><strong>Flood Unknown</strong></td>
<td>Whether the flooding of initial unknown multicast traffic is <strong>Enabled</strong> or <strong>Disabled</strong> (the default status). Configured through the <code>ipv6 multicast flood-unknown</code> command.</td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>Displays the default MLD version, which can be 1 or 2. Configured through the <code>ipv6 multicast version</code> command.</td>
</tr>
<tr>
<td><strong>Robustness</strong></td>
<td>Displays the MLD robustness value, ranging from 1 to 7. (The default value is 2). Configured through the <code>ipv6 multicast robustness</code> command.</td>
</tr>
<tr>
<td><strong>Querying</strong></td>
<td>Whether MLD querying is <strong>Enabled</strong> or <strong>Disabled</strong> (the default status). Configured through the <code>ipv6 multicast querying</code> command.</td>
</tr>
<tr>
<td><strong>Query Interval (seconds)</strong></td>
<td>Displays the time (in seconds) between MLD queries. (The default value is 125 seconds). Configured through the <code>ipv6 multicast query-interval</code> command.</td>
</tr>
<tr>
<td><strong>Query Response Interval (milliseconds)</strong></td>
<td>Displays the time (in milliseconds) taken to reply to an MLD query message. (The default value is 100 tenths-of-seconds). Configured through the <code>ipv6 multicast query-response-interval</code> command.</td>
</tr>
</tbody>
</table>
### Last Member Query Interval (milliseconds)
Displays the time (in milliseconds) taken to reply to an MLD query message sent in response to a leave group message. (The default value is 10 tenths-of-seconds.) Configured through the `ipv6 multicast last-member-query-interval` command.

### Unsolicited Report Interval (seconds)
Displays the time period (in seconds) to proxy any changed MLD membership state. (The default value is 1 second). Configured through the `ipv6 multicast unsolicited-report-interval` command.

### Proxying
Whether MLD proxying on the system is **Enabled** or **Disabled** (the default status). Configured through the `ipv6 multicast proxying` command.

### Spoofing
Whether MLD spoofing on the system is **Enabled** or **Disabled** (the default status). Configured through the `ipv6 multicast spoofing` command.

### Zapping
Whether MLD zapping on the system is **Enabled** or **Disabled** (the default status). Configured through the `ipv6 multicast zapping` command.

### Querier Forwarding
Whether MLD querier forwarding on the system is **Enabled** or **Disabled** (the default status). Configured through the `ipv6 multicast querier-forwarding` command.

### Router Timeout (seconds)
Displays the MLD router timeout in seconds. (The default value is 90 seconds.) Configured through the `ipv6 multicast router-timeout` command.

### Source Timeout (seconds)
Displays the MLD source timeout in seconds. (The default value is 30 seconds.) Configured through the `ipv6 multicast source-timeout` command.

### Max-group
Displays the global maximum group limit that can be learned per VLAN instance. (The default value is 0 which means no limit is imposed). Configured through the `ipv6 multicast max-group` command.

### Max-group action
Displays the action taken when the maximum group limit has been exceeded, which can be **none**, **drop** or **replace**. Configured through the `ipv6 multicast max-group` command.

### Helper-address
Displays the destination IPv6 address of a relay host, where MLD host reports and Leave messages are to be sent. (By default, no Helper-address is configured.) *This function is supported only in the VLAN domain; service domain is not supported.*

### Static Querier Address
The Static Source IPv6 Address to be used when querying. (The default value of “::” indicates that this is not configured.) *This function is not supported.*

### Static Spoofing Address
The Static Source IPv6 Address to be used when spoofing. (The default value of “::” indicates that this is not configured.) Configured through the `ipv6 multicast spoofing static-source-ip` command.

### Zero-based Query
The current state of Zero-based Querying, which can be **disabled** or **enabled** (the default status). Configured through the `ipv6 multicast zero-based-query` command.

### Forward Mode
Displays the current IPv6 Forwarding mode (**asm**, **ssm**, **mac**, or **auto**). Configured through the `ipv6 multicast forward-mode` command.
Show IPv6 Multicast

**Output Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update Delay Interval</strong></td>
<td>Displays the amount of time (in milliseconds) between propagating IPMS state changes. (The default value is 0 milliseconds). Configured through the <code>ipv6 multicast update-delay-interval</code> command.</td>
</tr>
<tr>
<td><strong>SSM Mapping</strong></td>
<td>Whether Source Specific Multicast (SSM) mapping is enabled or disabled (the default). When enabled, Any Source Multicast (ASM) group memberships are translated into SSM group memberships. Configured through the <code>ipv6 multicast ssm-map</code> command. This function is not supported.</td>
</tr>
<tr>
<td><strong>Fast Join</strong></td>
<td>Whether the IP Multicast Switching fast join functionality is enabled or disabled (the default). When enabled, forwarding entries are automatically created in hardware as soon as group memberships are learned instead of waiting for the multicast traffic to reach the switch. Configured through the <code>ipv6 multicast fast-join</code> command.</td>
</tr>
<tr>
<td><strong>Initial Packet Buffering</strong></td>
<td>Whether Initial Packet Buffering is enabled or disabled (the default status). Configured through the <code>ipv6 multicast initial-packet-buffer admin-state</code> command. This function is supported only in the VLAN domain; service domain is not supported.</td>
</tr>
<tr>
<td><strong>Max Flows</strong></td>
<td>The maximum number of IPv6 multicast flows buffered for initial packet. Configured through the <code>ipv6 multicast initial-packet-buffer max-flow</code> command. This function is supported only in the VLAN domain; service domain is not supported.</td>
</tr>
<tr>
<td><strong>Max Packets Per Flow</strong></td>
<td>The maximum number of initial packets buffered per IPv6 multicast flow. Configured through the <code>ipv6 multicast initial-packet-buffer max-packet</code> command. This function is supported only in the VLAN domain; service domain is not supported.</td>
</tr>
<tr>
<td><strong>Buffer Timeout</strong></td>
<td>The timeout value for the initial buffered IPv6 multicast packets. Configured through the <code>ipv6 multicast initial-packet-buffer timeout</code> command. This function is supported only in the VLAN domain; service domain is not supported.</td>
</tr>
<tr>
<td><strong>Min Delay</strong></td>
<td>The minimum delay to program the multicast replication index for IPv6 multicast flows buffered for initial packet. Configured through the <code>ipv6 multicast initial-packet-buffer min-delay</code> command. This function is supported only in the VLAN domain; service domain is not supported.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1; display fields added.
Release 8.4.1; `service` parameter added.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 multicast admin-state</code></td>
<td>Enables or disables IPv6 Multicast Switching and Routing on the specified VLAN or on the system if no VLAN is specified.</td>
</tr>
</tbody>
</table>
**MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaIpmsConfigTable</td>
</tr>
<tr>
<td>alaIpmsConfigType</td>
</tr>
<tr>
<td>alaIpmsConfigAddressType</td>
</tr>
<tr>
<td>alaIpmsConfigValue</td>
</tr>
<tr>
<td>alaIpmsConfigStatus</td>
</tr>
<tr>
<td>alaIpmsConfigQuerying</td>
</tr>
<tr>
<td>alaIpmsConfigProxying</td>
</tr>
<tr>
<td>alaIpmsConfigSpoofing</td>
</tr>
<tr>
<td>alaIpmsConfigZapping</td>
</tr>
<tr>
<td>alaIpmsConfigQuerierForwarding</td>
</tr>
<tr>
<td>alaIpmsConfigVersion</td>
</tr>
<tr>
<td>alaIpmsConfigRobustness</td>
</tr>
<tr>
<td>alaIpmsConfigQueryInterval</td>
</tr>
<tr>
<td>alaIpmsConfigQueryResponseInterval</td>
</tr>
<tr>
<td>alaIpmsConfigLastMemberQueryInterval</td>
</tr>
<tr>
<td>alaIpmsConfigUnsolicitedReportInterval</td>
</tr>
<tr>
<td>alaIpmsConfigRouterTimeout</td>
</tr>
<tr>
<td>alaIpmsConfigSourceTimeout</td>
</tr>
<tr>
<td>alaIpmsConfigMaxGroupLimit</td>
</tr>
<tr>
<td>alaIpmsConfigMaxGroupExceedAction</td>
</tr>
<tr>
<td>alaIpmsConfigFloodUnknown</td>
</tr>
<tr>
<td>alaIpmsConfigMaxGroupLimit</td>
</tr>
<tr>
<td>alaIpmsConfigMaxGroupExceedAction</td>
</tr>
<tr>
<td>alaIpmsConfigHelperAddress</td>
</tr>
<tr>
<td>alaIpmsConfigZeroBasedQuery</td>
</tr>
<tr>
<td>alaIpmsConfigInitialPacketBuffer</td>
</tr>
<tr>
<td>alaIpmsConfigDisplayInterfaceNames</td>
</tr>
<tr>
<td>alaIpmsConfigUpdateDelayInterval</td>
</tr>
<tr>
<td>alaIpmsConfigForwardMode</td>
</tr>
<tr>
<td>alaIpmsConfigQueryingStaticSourceAddress</td>
</tr>
<tr>
<td>alaIpmsConfigSpoofingStaticSourceAddress</td>
</tr>
</tbody>
</table>
**show ipv6 multicast port**

Displays the maximum group configuration applicable for the specified port or the specified Service Access Point (SAP) port. The current number of groups learned on a port, port/VLAN, SAP port, or SAP port/Shortest Path Bridging (SPB) service instance is also displayed.

*show ipv6 multicast {port [chassis/slot/port] | sap port [sap_id]}*

---

**Syntax Definitions**

- **chassis**
  The chassis identifier.

- **slot/port**
  The slot and port number (3/1).

- **sap_id**
  The SAP ID (chassis/slot/port:encapsulation). *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Specify a port number to display the configuration information for a specific port.

- Specify a SAP ID to display the configuration information for a specific SAP port.

- When using the `sap port` parameter with this command, specify a SAP ID by entering the access port number followed by the encapsulation value (for example, `ip multicast static-querier service 10 sap port 1/1/23:10`, where `1/1/23:10` is the SAP ID).

- A SAP ID is comprised of an access port and an encapsulation value. For example, the SAP ID for access port `1/1/23` with VLAN `10` encapsulation is `1/1/23:10`. Any traffic received on port `1/1/23` that is tagged with VLAN `10` is mapped to the SPB service that is associated with the `1/1/23:10` SAP ID. Refer to Chapter 10, “Service Manager Commands,” for more information.
Examples

-> show ipv6 multicast port

Legends: Interface Max-group = Max-group limit on the interface
        Interface Action = Max-group action on the interface
        Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
        Interface-Instance Action = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Interface Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/4/38</td>
<td>vlan 1001</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>1/5/43</td>
<td>vlan 1002</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>1/6/23</td>
<td>vlan 1003</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast port 1/6/23

Legends: Interface Max-group = Max-group limit on the interface
        Interface Action = Max-group action on the interface
        Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
        Interface-Instance Action = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Interface Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/5:100</td>
<td>service 20</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>sap:1/1/23:200</td>
<td>service 30</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>sap:1/3/10:14</td>
<td>service 10</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast sap port

Legends: Interface Max-group = Max-group limit on the interface
        Interface Action = Max-group action on the interface
        Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
        Interface-Instance Action = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Interface Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/5:100</td>
<td>service 20</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>sap:1/1/23:200</td>
<td>service 30</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
<tr>
<td>sap:1/3/10:14</td>
<td>service 10</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast sap port 1/1/23:200

Legends: Interface Max-group = Max-group limit on the interface
        Interface Action = Max-group action on the interface
        Interface-Instance Max-group = Active Max-group limit on the Lan Interface instance
        Interface-Instance Action = Active Max-group action on the Lan Interface instance

Total 1 Lan Interface Instances

<table>
<thead>
<tr>
<th>Interface</th>
<th>Vlan/Service</th>
<th>Current Groups</th>
<th>Interface Max-group</th>
<th>Interface Action</th>
<th>Interface-Instance Max-group</th>
<th>Interface-Instance Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap:1/1/23:200</td>
<td>service 30</td>
<td>0</td>
<td>0</td>
<td>none</td>
<td>0</td>
<td>none</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Interface</th>
<th>The VLAN port or the SAP (chassis/slot/port:encapsulation) that serves as the virtual port for the SPB service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan/Service</td>
<td>The VLAN or SPB service ID associated with the IPv6 multicast interface.</td>
</tr>
<tr>
<td>Current Groups</td>
<td>The current groups associated with the IPv6 multicast interface.</td>
</tr>
<tr>
<td>Interface Max-group</td>
<td>The maximum group count allowed on the port or SAP port. This limit is applicable on the given port for all VLAN or service instances of the port.</td>
</tr>
<tr>
<td>Interface Action</td>
<td>The action to be taken when the group membership limit is exceeded (none, drop, or replace).</td>
</tr>
<tr>
<td>Interface-Instance Max-group</td>
<td>The maximum group limit learned per port for the given VLAN or per SPB service. This limit is applied to each port that is a member of the given VLAN or each SAP port that is a member of the given service.</td>
</tr>
<tr>
<td>Interface-Instance Action</td>
<td>The action to be taken when the group membership limit is exceeded (none, drop, or replace).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; sap port parameter added.

**Related Commands**

- **ipv6 multicast port max-group** Configures the maximum group limit learned per port.
- **ipv6 multicast max-group** Configures the maximum group limit learned per port for the specified VLAN, SPB service, or on the system if no VLAN or SPB service is specified.

**MIB Objects**

- alaIpmsIntfStatsConfigType
  - alaIpmsIntfStatsAddressType
  - alaIpmsIntfStatsValue
  - alaIpmsIntfStatsCurrentGroupCount
  - alaIpmsIntfStatsMaxGroupLimit
  - alaIpmsIntfStatsMaxGroupExceedAction
**show ipv6 multicast forward**

Display the IPv6 Multicast Switching and Routing forwarding table entries for the specified IPv6 multicast group address or all entries if no IPv6 multicast address is specified.

```
show ipv6 multicast forward [ipv6_address] [vlan [vlan_id]-[vlan_id2]] [service [service_id]-[service_id2]] [all-vrf]
```

**Syntax Definitions**

- `ipv6_address` IPv6 multicast group address.
- `vlan [vlan_id]-[vlan_id2]` Display forwarding table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- `service [service_id]-[service_id2]` Display forwarding table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `all-vrf` Display forwarding table entries for all of the VRF instances.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `ipv6_address` parameter to display forwarding entries for a specific multicast group.
- Use the `all-vrf` parameter option to display the forwarding table entries that exist in all of the VRF instances on the switch.
- Forwarding entries are derived by applying the state from the source table to the state in the group, neighbor, and querier tables.
- On an OmniSwitch 9900, this command is available only when IP Multicast Switching and Routing is enabled for the switch. To view the multicast forwarding database on an OmniSwitch 6465 or OmniSwitch 6560 or OmniSwitch 6570M, see the `show ipv6 multicast bridge` and `show ipv6 multicast bridge-forward` commands.
- Use the `ipv6 multicast display-interface-names` command to enable displaying the associated IPv6 interface name in the “Ingress Vlan/Service” and “Egress Vlan/Service” fields instead of the VLAN ID or service ID.
Examples

-> show ipv6 multicast forward

Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>VLAN/Service</th>
<th>Egress VLAN/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 20</td>
<td>vlan 20</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 20</td>
<td>vlan 20</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
<td>vlan 21</td>
<td>1/1/2</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast forward ff05::6

Total 1 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>VLAN/Service</th>
<th>Egress VLAN/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 20</td>
<td>vlan 20</td>
<td>1/1/2</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast forward service

Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>VLAN/Service</th>
<th>Egress VLAN/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>service 10</td>
<td>service 10</td>
<td>sdp:32776</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>service 10</td>
<td>service 10</td>
<td>sdp:32776</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>service 10</td>
<td>service 10</td>
<td>sap:1/5:10</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast forward vlan

Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>VLAN/Service</th>
<th>Egress VLAN/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 20</td>
<td>vlan 20</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 20</td>
<td>vlan 20</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
<td>vlan 21</td>
<td>1/1/2</td>
</tr>
</tbody>
</table>

Sample output when the global display interface names option is enabled:

-> ip multicast display-interface-names

-> show ipv6 multicast forward vlan

Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>VLAN/Service</th>
<th>Egress VLAN/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>VlanToLab</td>
<td>VlanToLab</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>VlanToLab</td>
<td>VlanToLab</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>VlanToCore</td>
<td>VlanToDist</td>
<td>1/1/2</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Group Address</th>
<th>IPv6 group address of the IPv6 multicast forward.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>IPv6 host address of the IPv6 multicast forward.</td>
</tr>
<tr>
<td>Tunnel Address</td>
<td>IPv6 source tunnel address of the IPv6 multicast forward.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1; `all-vrf` parameter added.
Release 8.4.1; `domain` parameter added.
Release 8.4.1.R02; `domain` parameter deprecated.

**Related Commands**

`ipv6 multicast static-group`  
Creates a static MLD group entry on a specified port on a specified VLAN.

**MIB Objects**

- `alaIpmsForwardTable`
- `alaIpmsForwardConfigType`
- `alaIpmsForwardAddressType`
- `alaIpmsForwardValue`
- `alaIpmsForwardGroupAddress`
- `alaIpmsForwardHostAddress`
- `alaIpmsForwardDestAddress`
- `alaIpmsForwardOrigAddress`
- `alaIpmsForwardType`
- `alaIpmsForwardNextConfigType`
- `alaIpmsForwardNextValue`
- `alaIpmsForwardNextIfIndex`
- `alaIpmsForwardNextType`
show ipv6 multicast neighbor

Displays the MLD neighbor table entries of IPv6 Multicast Switching and Routing.

show ipv6 multicast neighbor [vlan [vlan_id]-vlan_id2] [service [service_id]-service_id2]] [all-vrf]

Syntax Definitions

- **vlan [vlan_id]-vlan_id2** Display MLD neighbor table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- **service [service_id]-service_id2** Display MLD neighbor table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **all-vrf** Display MLD neighbor table entries for all of the VRF instances.

Defaults

By default, only the neighbor table entries specific to the current VRF instance are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **all-vrf** parameter option to display the IPv6 neighbor table entries that exist in all of the VRF instances on the switch.
- Interfaces with neighbors receive all IPv6 multicast, including all MLD traffic.
- Use the **ipv6 multicast display-interface-names** command to enable displaying the associated IPv6 interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```bash
-> show ipv6 multicast neighbor

Total 4 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853</td>
<td>vlan 20</td>
<td>1/1/2</td>
<td>no</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>fe80::2a0:ccff:fed3:2853</td>
<td>service 20</td>
<td>SAP:1/5:10</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
<tr>
<td>::</td>
<td>vlan 20</td>
<td>1/1/13</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>::</td>
<td>service 20</td>
<td>SAP:1/5:20</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
</tbody>
</table>
```
-> show ipv6 multicast neighbor service

Total 2 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853</td>
<td>service 20</td>
<td>SAP:1/5:10</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
<tr>
<td>::</td>
<td>service 20</td>
<td>SAP:1/5:20</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast neighbor vlan

Total 2 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853</td>
<td>vlan 20</td>
<td>1/1/2</td>
<td>no</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>::</td>
<td>vlan 20</td>
<td>1/1/13</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Sample output when the global display interface names option is enabled:

-> ipv6 multicast display-interface-names
-> show ipv6 multicast neighbor vlan

Total 2 Neighbors

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853</td>
<td>VlanToLab</td>
<td>1/1/2</td>
<td>no</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>::</td>
<td>VlanToLab</td>
<td>1/1/13</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Address</strong></td>
<td>The IPv6 address of the IPv6 multicast neighbor.</td>
</tr>
<tr>
<td><strong>VLAN/Service</strong></td>
<td>The VLAN or Shortest Path Bridging (SPB) service ID associated with the IPv6 multicast neighbor. If the global display interface names option is enabled, then the interface name associated with the IP multicast neighbor is displayed.</td>
</tr>
<tr>
<td><strong>Interface</strong></td>
<td>The VLAN port or the SPB virtual port of the IPv6 multicast neighbor.</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td>Whether it is a static MLD neighbor or not.</td>
</tr>
<tr>
<td><strong>Count</strong></td>
<td>Displays the count of the IPv6 multicast neighbor.</td>
</tr>
<tr>
<td><strong>Life</strong></td>
<td>The life time of the IPv6 multicast neighbor.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1; **all-vrf** parameter added.
Release 8.4.1; **domain** parameter added.
Release 8.4.1.R02; **domain** parameter deprecated.
**Related Commands**

ipv6 multicast static-neighbor  Creates a static MLD neighbor entry on a specified port on a specified VLAN.

**MIB Objects**

alaIpmsNeighborTable
  alaIpmsNeighborConfigType
  alaIpmsNeighborAddressType
  alaIpmsNeighborValue
  alaIpmsNeighborIfIndex
  alaIpmsNeighborHostAddress
  alaIpmsNeighborCount
  alaIpmsNeighborTimeout
  alaIpmsNeighborUpTime
alaIpmsStaticNeighborTable
  alaIpmsStaticNeighborConfigType
  alaIpmsStaticNeighborAddressType
  alaIpmsStaticNeighborValue
  alaIpmsStaticNeighborIfIndex
  alaIpmsStaticNeighborRowStatus
**show ipv6 multicast querier**

Displays the MLD querier table entries of IPv6 Multicast Switching and Routing.

```plaintext
show ipv6 multicast querier [vlan [vlan_id]-vlan_id2] [service [service_id]-service_id2]] [all-vrf]
```

**Syntax Definitions**

- `vlan [vlan_id]-vlan_id2` Display MLD querier table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- `service [service_id]-service_id2` Display MLD querier table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `all-vrf` Display querier table entries for all of the VRF instances.

**Defaults**

By default, only MLD querier entries specific to the current VRF instance are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `all-vrf` parameter option to display the MLD querier table entries that exist in all of the VRF instances on the switch.
- Interfaces with queriers receive all MLD traffic, and if querier forwarding is enabled, these interfaces will also receive all IPv6 multicast traffic.
- Use the `ipv6 multicast display-interface-names` command to enable displaying the associated IPv6 interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

**Examples**

```plaintext
-> show ipv6 multicast querier

Total 4 Queriers

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853</td>
<td>vlan 20</td>
<td>1/1/2</td>
<td>no</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>fe80::2a0:ccff:fed3:2853</td>
<td>service 20</td>
<td>SAP:1/5:10</td>
<td>no</td>
<td>5520</td>
<td>172</td>
</tr>
<tr>
<td>::</td>
<td>vlan 20</td>
<td>1/1/13</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show ipv6 multicast querier

Output:

```
:: service 20 SAP:1/5:20 no 5520 172

-> show ipv6 multicast querier service

Total 2 Queriers

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853 service 20 SAP:1/5:10</td>
<td>no 5520 172</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>:: service 20 SAP:1/5:20</td>
<td>no 5520 172</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-> show ipv6 multicast querier vlan

Total 2 Queriers

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853 vlan 20 1/1/2</td>
<td>no 1 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>:: vlan 20 1/1/13</td>
<td>yes 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sample output when the global display interface names option is enabled:

-> ipv6 multicast display-interface-names

-> show ipv6 multicast querier vlan

Total 2 Queriers

<table>
<thead>
<tr>
<th>Host Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>fe80::2a0:ccff:fed3:2853 VlanToLab 1/1/2</td>
<td>no 1 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>:: VlanToLab 1/1/13</td>
<td>yes 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Output Definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Address</td>
<td>The IPv6 address of the IPv6 multicast querier.</td>
</tr>
<tr>
<td>VLAN/Service</td>
<td>The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast querier. If the global display interface names option is enabled, then the IPv6 interface name associated with the IPv6 multicast querier is displayed.</td>
</tr>
<tr>
<td>Interface</td>
<td>The VLAN port or the SPB virtual port of the IPv6 multicast querier.</td>
</tr>
<tr>
<td>Static</td>
<td>Whether it is a static MLD neighbor or not.</td>
</tr>
<tr>
<td>Count</td>
<td>Displays the count of the IPv6 multicast querier.</td>
</tr>
<tr>
<td>Life</td>
<td>The life time of the IPv6 multicast querier.</td>
</tr>
</tbody>
</table>

**Release History**

- Release 7.1.1; command was introduced
- Release 8.3.1; all-vrf parameter added.
- Release 8.4.1; domain parameter added.
- Release 8.4.1.R02; domain parameter deprecated.
Related Commands

**ipv6 multicast static-querier** Creates a static MLD querier entry on a specified port on a specified VLAN.

MIB Objects

alaIpmsQuerierTable
  - alaIpmsQuerierConfigType
  - alaIpmsQuerierAddressType
  - alaIpmsQuerierValue
  - alaIpmsQuerierIfIndex
  - alaIpmsQuerierHostAddress
  - alaIpmsQuerierCount
  - alaIpmsQuerierTimeout
  - alaIpmsQuerierUpTime

alaIpmsStaticQuerierTable
  - alaIpmsStaticQuerierConfigType
  - alaIpmsStaticQuerierAddressType
  - alaIpmsStaticQuerierValue
  - alaIpmsStaticQuerierIfIndex
  - alaIpmsStaticQuerierRowStatus
show ipv6 multicast group

Displays the MLD group membership table entries of IPv6 Multicast Switching and Routing for the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

show ipv6 multicast group [ipv6_address] [vlan [vlan_id[-vlan_id2]] | service [service_id[-service_id2]]] [all-vrf]

Syntax Definitions

ipv6_address IPv6 multicast group address.

vlan [vlan_id[-vlan_id2]] Display MLD group membership entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.

service [service_id[-service_id2]] Display MLD group membership entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*

all-vrf Display group membership entries for all of the VRF instances.

Defaults

By default, all IPv6 multicast groups are displayed for the current VRF instance.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `ipv6_address` parameter to display entries for a specific multicast group.
- Use the `all-vrf` parameter option to display the MLD group membership table entries that exist in all of the VRF instances on the switch.
- Use the `ipv6 multicast display-interface-names` command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

```
-> show ipv6 multicast group ff05::5

Group Address   Source Address Vlan/Service Interface Mode Static Count Life
-----------------------------------------------+-----------------+------------+--------+-------------+--------+------
ff05::5         ::             vlan 21      1/1/19     exclude  no     1      145
```
**IP Multicast Switching Commands**

```
ff05::5 :: service 20 SAP:1/5:10 exclude no 5520 172

-> show ipv6 multicast group service

Total 3 Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::5</td>
<td>::</td>
<td>service 20</td>
<td>1/1/19</td>
<td>exclude</td>
<td>no</td>
<td>100</td>
<td>145</td>
</tr>
<tr>
<td>ff05::6</td>
<td>::</td>
<td>service 20</td>
<td>1/1/19</td>
<td>exclude</td>
<td>no</td>
<td>100</td>
<td>145</td>
</tr>
<tr>
<td>ff05::7</td>
<td>::</td>
<td>service 20</td>
<td>1/1/19</td>
<td>exclude</td>
<td>no</td>
<td>101</td>
<td>145</td>
</tr>
<tr>
<td>ff05::8</td>
<td>::</td>
<td>vlan 100</td>
<td>1/1/20</td>
<td>exclude</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ff05::9</td>
<td>::</td>
<td>vlan 101</td>
<td>1/1/21</td>
<td>exclude</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Sample output when the global display interface names option is enabled:

-> ipv6 multicast display-interface-names

-> show ipv6 multicast group vlan

Total 3 Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
<th>Mode</th>
<th>Static</th>
<th>Count</th>
<th>Life</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::5</td>
<td>::</td>
<td>VlanToLab</td>
<td>1/1/19</td>
<td>exclude</td>
<td>no</td>
<td>100</td>
<td>145</td>
</tr>
<tr>
<td>ff05::6</td>
<td>::</td>
<td>VlanToLab</td>
<td>1/1/19</td>
<td>exclude</td>
<td>no</td>
<td>100</td>
<td>145</td>
</tr>
<tr>
<td>ff05::7</td>
<td>::</td>
<td>VlanToLab</td>
<td>1/1/19</td>
<td>exclude</td>
<td>no</td>
<td>101</td>
<td>145</td>
</tr>
<tr>
<td>ff05::8</td>
<td>::</td>
<td>VlanToCore</td>
<td>1/1/20</td>
<td>exclude</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ff05::9</td>
<td>::</td>
<td>VlanToDist</td>
<td>1/1/21</td>
<td>exclude</td>
<td>yes</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**output definitions**

| Group Address | IPv6 address of the IPv6 multicast group. |
| Source Address| IPv6 address of the IPv6 multicast source. |
| Vlan/Service  | The VLAN or Shortest Path Bridging (SPB) service ID associated with the IPv6 multicast group. If the global display interface names option is enabled, then the IPv6 interface name associated with the IPv6 multicast group is displayed. |
| Interface     | The VLAN port or the SPB virtual port on which the group membership was learned. |
| Mode          | MLD source filter mode. |
| Static        | Whether it is a static MLD group or not. |
| Count         | Number of MLD membership requests made. |
| Life          | Life time of the MLD group membership. |
Release History

Release 7.1.1; command was introduced
Release 8.3.1; all-vrf parameter added.
Release 8.4.1; domain parameter added.
Release 8.4.1.R02; domain parameter deprecated.

Related Commands

ipv6 multicast static-group  Creates a static MLD group entry on a specified port for the specified VLAN or on the specified SPB virtual port for the specified SPB service.

MIB Objects

alaIpmsMemberTable
  alaIpmsMemberConfigType
  alaIpmsMemberAddressType
  alaIpmsMemberValue
  alaIpmsMemberIfIndex
  alaIpmsMemberGroupAddress
  alaIpmsMemberSourceAddress
  alaIpmsMemberMode
  alaIpmsMemberCount
  alaIpmsMemberTimeout
alaIpmsStaticMemberTable
  alaIpmsStaticMemberConfigType
  alaIpmsStaticMemberConfigAddressType
  alaIpmsStaticMemberValue
  alaIpmsStaticMemberIfIndex
  alaIpmsStaticMemberGroupAddress
  alaIpmsStaticMemberRowStatus
show ipv6 multicast source

Displays the IPv6 Multicast Switching and Routing source table entries matching the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified.

**Syntax Definitions**

- `ipv6_address`: IPv6 multicast group address.
- `vlan [vlan_id]-vlan_id2`: Display source table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- `service [service_id]-service_id2`: Display source table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- `all-vrf`: Displays source table entries for all of the VRF instances.

**Defaults**

By default, all source table entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `ipv6_address` parameter to display entries for a specific multicast group.
- Use the `all-vrf` parameter option to display the MLD source table entries that exist in all of the VRF instances on the switch.
- On an OmniSwitch 9900, this command is available only when IP Multicast Switching and Routing is enabled for the switch. To view the multicast forwarding database on an OmniSwitch 6465 or OmniSwitch 6560 or OmniSwitch 6570M, see the `show ip multicast bridge` and `show ip multicast bridge-forward` commands.
- Use the `ipv6 multicast display-interface-names` command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.
## Examples

`-> show ipv6 multicast source`

Total 8 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 21</td>
</tr>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>service 20</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 21</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>service 20</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>service 21</td>
</tr>
<tr>
<td>ff06::2</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
</tr>
<tr>
<td>ff06::2</td>
<td>::</td>
<td>::</td>
<td>service 21</td>
</tr>
</tbody>
</table>

`-> show ipv6 multicast source ff05::6`

Total 2 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 21</td>
</tr>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>service 20</td>
</tr>
</tbody>
</table>

`-> show ipv6 multicast source service`

Total 4 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>service 20</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>service 20</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>service 21</td>
</tr>
<tr>
<td>ff06::2</td>
<td>::</td>
<td>::</td>
<td>service 21</td>
</tr>
</tbody>
</table>

`-> show ipv6 multicast source vlan`

Total 4 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source</th>
<th>Ingress</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 21</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>vlan 21</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
</tr>
<tr>
<td>ff06::2</td>
<td>::</td>
<td>::</td>
<td>vlan 20</td>
</tr>
</tbody>
</table>
Sample output when the global display interface names option is enabled:

```
-> ipv6 multicast display-interface-names
-> show ipv6 multicast source vlan

Total 4 Sources

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Source Tunnel Address</th>
<th>Ingress VLAN/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>VlanToLab</td>
</tr>
<tr>
<td>ff06::1</td>
<td>::</td>
<td>::</td>
<td>VlanToCore</td>
</tr>
<tr>
<td>ff06::2</td>
<td>::</td>
<td>::</td>
<td>VlanToCore</td>
</tr>
</tbody>
</table>
```

**output definitions**

- **Group Address**: IPv6 group address of the IPv6 multicast source.
- **Host Address**: IPv6 host address of the IPv6 multicast source.
- **Source Tunnel Address**: IPv6 source tunnel address of the IPv6 multicast source.
- **Ingress VLAN/Service**: The ingress VLAN or Shortest Path Bridging (SPB) service ID number associated with the IP multicast source. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast source is displayed.

**Release History**

- Release 7.1.1; command was introduced.
- Release 8.3.1; **all-vrf** parameter added.
- Release 8.4.1; **domain** parameter added.
- Release 8.4.1.R02; **domain** parameter deprecated.

**Related Commands**

- **show ipv6 multicast tunnel**: Display the IP Multicast Switching and Routing tunneling table entries matching the specified IP multicast group address or all entries if no IP multicast address is specified.

**MIB Objects**

- alaIpmsSourceTable
  - alaIpmsSourceConfigType
  - alaIpmsSourceAddressType
  - alaIpmsSourceValue
  - alaIpmsSourceGroupAddress
  - alaIpmsSourceHostAddress
  - alaIpmsSourceDestAddress
  - alaIpmsSourceOrigAddress
  - alaIpmsSourceType
  - alaIpmsSourceUpTime
**show ipv6 multicast tunnel**

Displays the IPv6 Multicast Switching and Routing tunneling table entries matching the specified IPv6 multicast group address, or all entries if no IPv6 multicast address is specified.

```
show ipv6 multicast tunnel [ipv6_address] [vlan [vlan_id1]-vlan_id2] | service [service_id1]-service_id2] [all-vrf]
```

**Syntax Definitions**

- `ipv6_address` IPv6 multicast group address.
- `vlan [vlan_id1]-vlan_id2` Display tunneling table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- `service [service_id1]-service_id2` Display tunneling table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.
- `all-vrf` Display the IPv6 tunneling table entries for all of the VRF instances.

**Defaults**

By default, all IPv6 tunnel entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `ip_address` parameter to display the tunnel entries for a specific multicast group.
- Use the `all-vrf` parameter option to display the IPv6 multicast tunnel entries that exist in all of the VRF instances on the switch.
- Use the `ipv6 multicast display-interface-names` command to enable displaying the associated IP interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

**Examples**

```
-> show ipv6 multicast tunnel

Total 4 Tunnels

Destination Ingress
Group Address Host Address Tunnel Address Vlan/Service
```
### show ipv6 multicast tunnel

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Host Address</th>
<th>Tunnel Address</th>
<th>Ingress Vlan/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>4444::2</td>
<td>::</td>
<td>service 20</td>
</tr>
<tr>
<td>ff05::7</td>
<td>4444::2</td>
<td>::</td>
<td>service 20</td>
</tr>
</tbody>
</table>

Total 2 Tunnels

Sample output when the global display interface names option is enabled:

```bash
- show ipv6 multicast display-interface-names
- show ipv6 multicast tunnel vlan
```

```bash
- show ipv6 multicast tunnel service
```

### output definitions

- **Group Address**: IPv6 group address of the IPv6 multicast tunnel.
- **Host Address**: IPv6 host address of the IPv6 multicast tunnel.
- **Destination Tunnel Address**: IPv6 source tunnel address of the IPv6 multicast tunnel.
- **Ingress Vlan/Service**: VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast tunnel. If the global display interface names option is enabled, then the IP interface name associated with the IP multicast tunnel is displayed.

### Release History

- Release 7.1.1; command was introduced.
- Release 8.3.1; **all-vrf** parameter added.
- Release 8.4.1.R02; **vlan** and **service** parameters added.
Related Commands

**show ipv6 multicast source** Displays the IPv6 Multicast Switching and Routing source table entries matching the specified IPv6 multicast group address or all entries if no IPv6 multicast group address is specified

MIB Objects

alaIpmsTunnelTable
  alaIpmsTunnelConfigType
  alaIpmsTunnelAddressType
  alaIpmsTunnelValue
  alaIpmsTunnelGroupAddress
  alaIpmsTunnelHostAddress
  alaIpmsTunnelDestAddress
  alaIpmsTunnelOrigAddress
  alaIpmsTunnelType
  alaIpmsTunnelNextDestAddress
  alaIpmsTunnelNextType
**show ipv6 multicast host-list**

Displays the IPv6 multicast host address list configuration for the switch.

```
show ipv6 multicast host-list [host_list_name]
```

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th><code>host_list_name</code></th>
<th>The name of an existing IPv6 multicast host list.</th>
</tr>
</thead>
</table>

---

**Defaults**

By default, all host lists configured on the switch are displayed.

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

Use the `host_list_name` parameter to display information for a specific host list.

**Examples**

```
-> show ipv6 multicast host-list

Total 2 Lists

<table>
<thead>
<tr>
<th>Host List Name</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-map1</td>
<td>3333::2</td>
</tr>
<tr>
<td></td>
<td>3333::3</td>
</tr>
<tr>
<td></td>
<td>3333::4</td>
</tr>
<tr>
<td>ssm-map1</td>
<td>4444::2</td>
</tr>
<tr>
<td></td>
<td>4444::3</td>
</tr>
<tr>
<td></td>
<td>4444::4</td>
</tr>
</tbody>
</table>

-> show ipv6 multicast host-list ssm-map1

<table>
<thead>
<tr>
<th>Host List Name</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>ssm-map1</td>
<td>4444::2</td>
</tr>
<tr>
<td></td>
<td>4444::3</td>
</tr>
<tr>
<td></td>
<td>4444::4</td>
</tr>
</tbody>
</table>
```

**Release History**

Release 8.3.1.R02; command introduced.
Related Commands

**ipv6 multicast host-list**  
Configures a list of host IPv6 addresses that is used for IPv6 multicast group maps and SSM maps.

MIB Objects

*alaIpmsHostListTable*
  *alaIpmsHostListName*
  *alaIpmsHostListAddressType*
  *alaIpmsHostListAddress*
show ipv6 multicast ssm-map

Displays the IPv6 Source Specific Multicast (SSM) mapping configuration for the switch.

show ipv6 multicast ssm-map [vlan vlan_id]

Syntax Definitions

`vlan_id` VLAN for which to display the configuration.

Defaults

By default, all IPv6 multicast SSM mappings configured on the switch are displayed.

Platforms Supported

Not supported in this release.

Usage Guidelines

Specify a VLAN ID to display the configuration information for a specific VLAN.

Examples

```
-> show ipv6 multicast ssm-map
  Type   Id    Group Address/Prefix  Source List Name
  ------------------+----------------------------------
  global  0     ff05::5/128           h-list1
  vlan    200   ff05::6/128           h-list2

-> show ipv6 multicast ssm-map vlan 200
  Type   Id    Group Address/Prefix  Source List Name
  ------------------+----------------------------------
  vlan    200   ff05::6/128           h-list2
```

Release History

Release 8.3.1.R02; command introduced.

Related Commands

ipv6 multicast ssm-map Configures a list of host IP addresses that is used for IP multicast group maps and SSM maps.

MIB Objects

alaIpmsSsmMapTable
  alaIpmsSsmMapConfigType
  alaIpmsSsmMapConfigAddressType
  alaIpmsSsmMapConfigValue
  alaIpmsSsmMapGroupAddress
  alaIpmsSsmMapGroupPrefixLength
  alaIpmsSsmMapSourceListName
**show ipv6 multicast bridge**

Displays the IPv6 multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IPv6 multicast group address, MAC address, or all entries if no additional parameters are specified.

```
show ipv6 multicast bridge [vlan vlan_id[-vlan_id2] | service [service_id[-service_id2] | ipv6_address | mac_address]] [all-vrf]
```

**Syntax Definitions**

- **vlan [vlan_id][-vlan_id2]** Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- **service [service_id[-service_id2]** Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **ipv6_address** IPv6 multicast group address.
- **mac_address** Group MAC address.
- **all-vrf** Display bridge table entries for all of the VRF instances.

**Defaults**

By default, all bridge table entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use one of the optional parameters (`vlan_id`, `service-id`, `ipv6_address`, `mac_address`) to display bridge table entries for a specific multicast group.
- Use the `all-vrf` parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC).
  - The “Host Address” field will display zero (MAC) or the IPv6 host address for the bridge entry (ASM or SSM).
**Examples**

`-> show ipv6 multicast bridge vlan 130`

Total 2 Bridge Entries

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>Type</th>
<th>Group Address</th>
<th>Host Address</th>
<th>Action</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 130</td>
<td>asm</td>
<td>ff05::6</td>
<td></td>
<td>forwarding</td>
<td>00h:00m:04s</td>
</tr>
<tr>
<td>service 10</td>
<td>mac</td>
<td>33-33-00-01-01-01</td>
<td></td>
<td>flooding</td>
<td>00h:00m:05s</td>
</tr>
</tbody>
</table>

**output definitions**

- **Vlan/Service**: The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.
- **Type**: The bridge type for the IPv6 multicast bridge entry (asm, ssm, mac). Configured through the `ipv6 multicast forward-mode` command.
- **Group Address**: If the bridge entry type is ASM or SSM, this field displays the destination IP group address; if the bridge entry type is MAC, this field displays the destination MAC address.
- **Host Address**: The source IPv6 host address (only applies to SSM bridge entries, otherwise this field is blank).
- **Action**: The current action taken for the bridge entry (forwarding or filtering).
- **UpTime**: The amount of time that has elapsed since the bridge entry was created.

**Release History**

Release 8.3.1; command introduced.
Release 8.4.1.R02; `service` parameter added.

**Related Commands**

- `show ipv6 multicast bridge-forward`: Displays the forwarding state of the IPv6 multicast bridge table entries.

**MIB Objects**

- `alaIpmsBridgeTable`
  - `alaIpmsBridgeConfigType`
  - `alaIpmsBridgeAddressType`
  - `alaIpmsBridgeValue`
  - `alaIpmsBridgeType`
  - `alaIpmsBridgeGroupAddress`
  - `alaIpmsBridgeHostAddress`
  - `alaIpmsBridgeUpTime`
  - `alaIpmsBridgeAction`
**show ipv6 multicast bridge-forward**

Displays the forwarding state of the IPv6 multicast bridge table entries that match the specified VLAN, Shortest Path Bridging (SPB) service, IPv6 multicast group address, MAC address, or all entries if no additional parameters are specified.

```
show ipv6 multicast bridge-forward [vlan vlan_id]-[vlan_id2] | service [service_id]-[service_id2] | ipv6_address | mac_address] [all-vrf]
```

**Syntax Definitions**

- **vlan [vlan_id]-[vlan_id2]** Displays bridge table entries for the VLAN domain. Optionally enter a VLAN ID or use a hyphen to specify a range of VLAN IDs.
- **service [service_id]-[service_id2]** Displays bridge table entries for the service domain. Optionally enter a service ID or use a hyphen to specify a range of service IDs. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, or OmniSwitch 6570M.*
- **ipv6_address** IPv6 multicast group address.
- **mac_address** Group MAC address.
- **all-vrf** Display bridge table entries for all of the VRF instances.

**Defaults**

By default, all bridge table entries are displayed for the current VRF instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use one of the optional parameters (*vlan_id, service_id, ipv6_address, mac_address*) to display forwarding information for a specific multicast group.
- Use the **all-vrf** parameter option to display the source table entries that exist in all of the VRF instances on the switch.
- Based on the forwarding mode set for the switch (ASM, SSM, or MAC):
  - The “Group Address” field will display either a multicast group address (ASM or SSM) or the MAC address for the multicast group (MAC). In the examples for this command, the forwarding mode is changed to MAC to show how the “Group Address” field changes.
  - The “Host Address” field will display zero (MAC) or the IPv6 host address for the bridge entry (ASM or SSM).
Examples

-> show ipv6 multicast bridge-forward vlan 130

Total 2 Bridge Forwarding Entries

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>Type</th>
<th>Group Address</th>
<th>Host Address</th>
<th>Next Interface</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 1</td>
<td>asm-partial</td>
<td>::1.1.2.3</td>
<td></td>
<td>1/4/12</td>
<td>00h:00m:10s</td>
</tr>
<tr>
<td>vlan 130</td>
<td>asm</td>
<td>33-33-ff-ff-ff-ff</td>
<td></td>
<td>1/4/12</td>
<td>00h:00m:07s</td>
</tr>
</tbody>
</table>

-> ipv6 multicast vlan 130 forward-mode mac
-> show ipv6 multicast bridge-forward vlan 130

Total 1 Bridge Forwarding Entries

<table>
<thead>
<tr>
<th>Vlan/Service</th>
<th>Type</th>
<th>Group Address</th>
<th>Host Address</th>
<th>Next Interface</th>
<th>UpTime</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan 130</td>
<td>mac</td>
<td>33-33-ff-ff-ff-ff</td>
<td></td>
<td>1/3/25</td>
<td>00h:00m:07s</td>
</tr>
</tbody>
</table>

output definitions

Vlan/Service: The VLAN or Shortest Path Bridging (SPB) service ID associated with the IP multicast bridge entry.

Type: The bridge entry type (asm, ssm, mac). Configured through the ipv6 multicast forward-mode command.

Group Address: If the bridge entry type is ASM or SSM, this field displays the destination IPv6 group address; if the bridge entry type is MAC, this field displays the destination MAC address.

Host Address: The source IPv6 host address (only applies to SSM bridge entries, otherwise this field is blank).

Next Interface: The destination interface for the bridge forwarding entry.

UpTime: The amount of time that has elapsed since the bridge forward entry was created.

Release History

Release 8.3.1; command introduced.
Release 8.4.1.R02; service parameter added.
Related Commands

**show ipv6 multicast bridge** Displays the IPv6 multicast bridge table entries.

MIB Objects

alaIpmsBridgeForwardTable

alaIpmsBridgeForwardConfigType, alaIpmsBridgeForwardAddressType, alaIpmsBridgeForwardValue, alaIpmsBridgeForwardType, alaIpmsBridgeForwardGroupAddress, alaIpmsBridgeForwardHostAddress, alaIpmsBridgeForwardNextIfIndex, alaIpmsBridgeForwardNextSubValue alaIpmsBridgeForwardUpTime
show ipv6 multicast bidir-forward

Displays the IPv6 multicast Bidirectional Protocol Independent Multicast (BIDIR-PIM) forwarding table entries for the specified IPv6 multicast group address or all the entries if no IPv6 multicast group address is specified.

show ipv6 multicast bidir-forward [ipv6_address] [all-vrf]

Syntax Definitions

- **ipv6_address**: IPv6 multicast group address.
- **all-vrf**: Display forwarding table entries for all of the VRF instances.

Defaults

By default, BIDIR-PIM forwarding entries for all of the IPv6 multicast groups are displayed for the current VRF instance.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `ipv6_address` parameter to display BIDIR-PIM forwarding table entries for a specific multicast group.
- Use the `all-vrf` parameter option to display the BIDIR-PIM forwarding table entries that exist in all of the VRF instances on the switch.
- Use the `ipv6 multicast display-interface-names` command to enable displaying the associated IPv6 interface name in the “Vlan/Service” field instead of the VLAN ID or service ID.

Examples

-> vrf vrf-1 show ipv6 multicast bidir-forward

VRF:vrf-1  Total 3 Forwards

<table>
<thead>
<tr>
<th>Egress</th>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ff05::6</td>
<td>vlan 30</td>
<td>1/2/1</td>
</tr>
<tr>
<td></td>
<td>ff05::8</td>
<td>vlan 31</td>
<td>1/2/2</td>
</tr>
</tbody>
</table>
show ipv6 multicast bidir-forward all-vrf

VRF:default  Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>vlan 20</td>
<td>1/1/1</td>
</tr>
<tr>
<td></td>
<td>vlan 20</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff05::8</td>
<td>vlan 21</td>
<td>1/1/2</td>
</tr>
</tbody>
</table>

VRF:vrf-1  Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>vlan 30</td>
<td>1/2/1</td>
</tr>
<tr>
<td></td>
<td>vlan 30</td>
<td>1/2/2</td>
</tr>
<tr>
<td>ff05::8</td>
<td>vlan 31</td>
<td>1/2/2</td>
</tr>
</tbody>
</table>

Sample output when the global display interface names option is enabled:

ipv6 multicast display-interface-names
vrf vrf-1 show ipv6 multicast bidir-forward

VRF:vrf-1  Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>IPv6ToCore2</td>
<td>1/2/1</td>
</tr>
<tr>
<td></td>
<td>IPv6ToCore2</td>
<td>1/2/2</td>
</tr>
<tr>
<td>ff05::8</td>
<td>IPv6ToLab2</td>
<td>1/2/2</td>
</tr>
</tbody>
</table>

show ipv6 multicast bidir-forward all-vrf

VRF:default  Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>vlanToCore1</td>
<td>1/1/1</td>
</tr>
<tr>
<td></td>
<td>vlanToCore1</td>
<td>1/1/2</td>
</tr>
<tr>
<td>ff05::8</td>
<td>vlanToLab1</td>
<td>1/1/2</td>
</tr>
</tbody>
</table>

VRF:vrf-1  Total 3 Forwards

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Vlan/Service</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff05::6</td>
<td>IPv6ToCore2</td>
<td>1/2/1</td>
</tr>
<tr>
<td></td>
<td>IPv6ToCore2</td>
<td>1/2/2</td>
</tr>
<tr>
<td>ff05::8</td>
<td>IPv6ToLab2</td>
<td>1/2/2</td>
</tr>
</tbody>
</table>

Output definitions:

<table>
<thead>
<tr>
<th>VRF</th>
<th>The VRF instance for the BIDIR route.</th>
</tr>
</thead>
</table>
| Group Address| IPv6 group address for the BIDIR route.
output definitions (continued)

<table>
<thead>
<tr>
<th><strong>Egress VLAN/Service</strong></th>
<th>The destination VLAN or Shortest Path Bridging (SPB) service for the BIDIR route. If the global display interface names option is enabled, then the IPv6 interface name associated with the BIDIR route is displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>Destination VLAN port or SPB virtual port for the BIDIR route.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

- `show ipv6 multicast bridge-forward` Displays the forwarding state of the IPv6 multicast bridge table entries.

**MIB Objects**

- `alaIpmsForwardTable` (Continued)
  - `alaIpmsForwardConfigType`
  - `alaIpmsForwardAddressType`
  - `alaIpmsForwardValue`
  - `alaIpmsForwardGroupAddress`
  - `alaIpmsForwardHostAddress`
  - `alaIpmsForwardDestAddress`
  - `alaIpmsForwardOrigAddress`
  - `alaIpmsForwardType`
  - `alaIpmsForwardNextConfigType`
  - `alaIpmsForwardNextValue`
  - `alaIpmsForwardNextIfIndex`
  - `alaIpmsForwardNextType`
show ipv6 multicast profile

Displays a list of available IPMS configuration profiles or the parameter settings for a specific profile.

**show ipv6 multicast profile [profile_name]**

**Syntax Definitions**

**profile_name**

The name of an existing IPMS profile.

**Defaults**

By default, a list of available profiles is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The specified profile name must already exist in the switch configuration.

**Examples**

-> show ipv6 multicast profile

Total 2 Profiles

Profile Name
-----------------------
default
IGMPv3 with Zapping

-> show ip multicast profile "IGMPv3 with Zapping"

Status = enabled,
Flood Unknown = none,
Version = 3,
Robustness = 0,
Querying = none,
Query Interval (seconds) = 0,
Query Response Interval (tenths of seconds) = 0,
Last Member Query Interval (tenths of seconds) = 0,
Unsolicited Report Interval (seconds) = 0,
Proxying = enabled,
Spoofing = none,
Zapping = enabled,
Querier Forwarding = none,
Router Timeout (seconds) = 0,
Source Timeout (seconds) = 0,
Max-group = 0,
Max-group action = none,
Helper-address = ::,
Static Querier Address = ::,
Static Spoofed Address = ::,
Zero-based Query = none,
Forward Mode = none,
Update Delay Interval (milliseconds) = 0,
SSM Mapping = none,
Fast Join = none,
Initial Packet Buffering = none,
    Max Flows = 0,
    Max Packets Per Flow = 0,
    Buffer Timeout (seconds) = 0,
    Min Delay (milliseconds) = 0

**Release History**

Release 8.4.1.R02; command was introduced.

**Related Commands**

**ipv6 multicast profile**
Defines an IPMS profile that is used to apply a pre-defined IPMS configuration.

**ipv6 multicast apply-profile**
Applies the specified IPMS profile to the specified IPMS instance.

**show ipv6 multicast**
Displays the profile assignment for the IPMS instance.

**MIB Objects**

alaIpmsProfileTable
    alaIpmsProfileAddressType
    alaIpmsProfileName
    alaIpmsProfileIndex
    alaIpmsProfileRowStatus
alaIpmsConfigTable
    alaIpmsConfigType
    alaIpmsConfigAddressType
    alaIpmsConfigValue
    alaIpmsConfigProfileName
This chapter includes CLI command descriptions for Distance Vector Multicast Routing Protocol (DVMRP), version 3.

DVMRPv3 is a dense-mode multicast routing protocol that enables routers to efficiently propagate IP multicast traffic through a network. Multicast traffic consists of a data stream that originates from a single source and is sent to hosts that have subscribed to that stream. Live video broadcasts, video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news services are examples of multicast traffic.

For more information about configuring DVMRP, see the applicable OmniSwitch AOS Release 8 Advanced Routing Configuration Guide.

MIB information for the DVMRP commands is as follows:

- **Filename**: ALCATEL-IND1-VIRTUALROUTER-MIB.mib  
  **Module**: alcatelIND1VirtualRouterMIB

- **Filename**: ALCATEL-IND1-DVMRP-MIB.mib  
  **Module**: alcatelIND1DVMRPMIB

- **Filename**: DVMRP-STD-MIB.mib  
  **Module**: dvmrpStdMIB

A summary of the available commands is listed here:

```
ip load dvmrp
ip dvmrp admin-state
ip dvmrp flash-interval
ip dvmrp graft-timeout
ip dvmrp interface
ip dvmrp interface metric
ip dvmrp interface mbr-default-information
ip dvmrp neighbor-interval
ip dvmrp neighbor-timeout
ip dvmrp prune-lifetime
ip dvmrp prune-timeout
ip dvmrp report-interval
ip dvmrp route-holddown
ip dvmrp route-timeout
ip dvmrp subord-default
show ip dvmrp
show ip dvmrp interface
show ip dvmrp neighbor
show ip dvmrp nexthop
show ip dvmrp prune
show ip dvmrp route
show ip dvmrp tunnel
```
**ip load dvmrp**

Dynamically loads DVMRP to memory.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command must be executed before DVMRP can be configured on the switch. In addition, DVMRP must be administratively enabled before you can run the protocol on the switch. For more information, refer to the `ip dvmrp admin-state` command on page 33-3.

**Examples**

```
-> ip load dvmrp
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip dvmrp admin-state`  Globally enables or disables DVMRP protocol on the switch.

**MIB Objects**

- `alaVrConfigTable`
  - `alaVrConfigDvmrpStatus`
**ip dvmrp admin-state**

Globally enables or disables DVMRP protocol on the switch.

`ip dvmrp admin-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Administratively enables DVMRP on the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Administratively disables DVMRP on the switch.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command must be set to `enable` before DVMRP can run on the switch. In addition, the `ip load dvmrp` command must be issued. For more information, refer to the `ip load dvmrp` command on page 33-2.

- To enable or disable DVMRP for a particular interface, refer to the `ip dvmrp interface` command on page 33-7.

**Examples**

- `-> ip dvmrp admin-state enable`
- `-> ip dvmrp admin-state disable`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip dvmrp interface**
  Enables or disables the DVMRP protocol on a specified interface.
- **ip load dvmrp**
  Dynamically loads DVMRP to memory.
- **show ip dvmrp**
  Displays global DVMRP parameters, including current status.

MIB Objects

- **alaDvmrpGlobalConfig**
- **alaDvmrpAdminStatus**
ip dvmrp flash-interval

Configures the minimum flash update interval value. The flash update interval defines how often routing table change messages are sent to neighboring DVMRP routers.

`ip dvmrp flash-interval seconds`

**Syntax Definitions**

`seconds` Specifies the interval value, in seconds (5–86400).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>5</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval value must be lower than the route report interval.

**Examples**

`-> ip dvmrp flash-interval 5`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip dvmrp` Displays global DVMRP parameters.

**MIB Objects**

- `alaDvmrpGlobalConfig`
- `alaDvmrpFlashUpdateInterval`
ip dvmrp graft-timeout

Configures the graft message retransmission value. The graft message retransmission value is the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor.

**ip dvmrp graft-timeout seconds**

---

**Syntax Definitions**

*seconds* Specifies the graft message retransmission value, in seconds (5–86400).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>5</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

-> ip dvmrp graft-timeout 5

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

*show ip dvmrp* Displays global DVMRP parameters.

---

**MIB Objects**

alaDvmrpGlobalConfig
alaDvmrpGraftRetransmission
**ip dvmrp interface**

Enables or disables the DVMRP protocol on a specified interface.

```
ip dvmrp interface {interface_name}
no ip dvmrp interface {interface_name}
```

**Syntax Definitions**

- `interface_name` The name of the interface.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **no** form of this command to delete an interface.

**Examples**

- `-> ip dvmrp interface vlan-10`
- `-> no ip dvmrp interface vlan-10`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip dvmrp admin-state` - Globally enables or disables the DVMRP protocol on the switch.
- `ip dvmrp interface metric` - Configures the distance metric for an interface, which is used to calculate distance vectors.
- `show ip dvmrp interface` - Displays information for all multicast-capable interfaces.

**MIB Objects**

- `dvmrpInterfaceTable`
  - `dvmrpInterfaceLocalAddress`
  - `dvmrpInterfaceStatus`
**ip dvmrp interface metric**

Configures the distance metric for an interface, which is used to calculate distance vectors. DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network.

`ip dvmrp interface interface_name metric value`

---

**Syntax Definitions**

- `interface_name` The name of the interface.
- `value` Specifies the metric value (1–31).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

DVMRP uses the distance metric value to determine the most cost-effective way to pass data through the network. The higher the distance metric value, the higher the cost.

**Examples**

```plaintext
-> ip dvmrp interface vlan-2 metric 1
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ip dvmrp interface**
Enables or disables the DVMRP protocol on a specified interface.

**show ip dvmrp interface**
Displays the DVMRP interface table.

MIB Objects

dvmrpInterfaceTable
  dvmrpInterfaceLocalAddress
  dvmrpInterfaceMetric
**ip dvmrp interface mbr-default-information**

Configures a DVMRP interface to advertise the default route for the interface. This command only applies when the local switch is operating in the Multicast Border Router (MBR) mode.

```plaintext
ip dvmrp interface interface_name mbr-default-information {enable | disable}
```

**Syntax Definitions**

- **interface_name**: The name of the interface.
- **enable**: Enables advertisement of the default route on the specified interface.
- **disable**: Disables advertisement of the default route on the specified interface.

**Defaults**

By default, advertising the default route is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Advertising a default route on the DVMRP interface provides a method for ensuring that sources inside the PIM domain can reach all routers inside the DVMRP domain.
- Make sure that the default route is not advertised on the MBONE.

**Examples**

```plaintext
-> ip dvmrp interface mbr-default-information enable
-> ip dvmrp interface mbr-default-information disable
```

**Release History**

Release 7.3.2; command was introduced.
Related Commands

- **ip dvmrp interface**: Enables or disables the DVMRP protocol on a specified interface.
- **show ip dvmrp interface**: Displays the DVMRP interface table.

MIB Objects

- **alaDvmrpIfAugTable**
- **alaDvmrpIfMbrDefaultInfoStatus**
**ip dvmrp neighbor-interval**

Configures the neighbor probe interval time. The neighbor probe interval time specifies how often probes are transmitted on DVMRP-enabled interfaces.

`ip dvmrp neighbor-interval seconds`

---

**Syntax Definitions**

`seconds` Specifies the probe interval time, in seconds (5–30).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>10</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

```
-> ip dvmrp neighbor-interval 10
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `ip dvmrp neighbor-timeout` Configures the neighbor timeout.
- `show ip dvmrp neighbor` Displays the DVMRP neighbor table.
- `show ip dvmrp` Displays the global DVMRP parameters.

---

**MIB Objects**

- `alaDvmrpGlobalConfig`
- `alaDvmrpNeighborProbeInterval`
**ip dvmrp neighbor-timeout**

Configures the neighbor timeout. This value specifies how long the switch will wait for activity from a neighboring DVMRP router before assuming that the inactive router is down.

`ip dvmrp neighbor-timeout seconds`

---

**Syntax Definitions**

`seconds` Specifies the neighbor timeout, in seconds (5–86400).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>35</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

```
-> ip dvmrp neighbor-timeout 35
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `ip dvmrp neighbor-interval` Configures the neighbor probe interval time.
- `show ip dvmrp neighbor` Displays the DVMRP neighbor table.
- `show ip dvmrp` Displays the global DVMRP parameters.

---

**MIB Objects**

- `alaDvmrpGlobalConfig`
- `alaDvmrpNeighborTimeout`
**ip dvmrp prune-lifetime**

Indicates the length of time a prune will be in effect—i.e., its *lifetime*. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue.

```
ip dvmrp prune-lifetime seconds
```

### Syntax Definitions

```
seconds
```

Specifies the prune lifetime, in seconds (180–86400).

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>7200</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> ip dvmrp prune-lifetime 7200
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `ip dvmrp prune-timeout` Configures the prune packet retransmission value.
- `show ip dvmrp prune` Displays DVMRP prune entries, including the router’s upstream prune state.
- `show ip dvmrp` Displays the global DVMRP parameters.

### MIB Objects

alaDvmrpGlobalConfig
DVMRP Commands

ip dvmrp prune-lifetime

alaDvmrpPruneLifetime
**ip dvmrp prune-timeout**

Configures the prune packet retransmission value. This value is the duration of time that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message.

**ip dvmrp prune-timeout seconds**

---

**Syntax Definitions**

*seconds* Specifies retransmission time, in seconds (30–86400).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>30</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

--> ip dvmrp prune-timeout 30

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip dvmrp prune-lifetime** Indicates the length of time a prune will be in effect.
- **show ip dvmrp prune** Displays DVMRP prune entries, including the router’s upstream prune state.
- **show ip dvmrp** Displays the global DVMRP parameters.

**MIB Objects**

alaDvmrpGlobalConfig
DVMRP Commands

ip dvmrp prune-timeout

alaDvmrpPruneRetransmission
ip dvmrp report-interval

Configures the route report interval. This value defines how often the switch will send its complete routing table to neighboring routers running DVMRP.

ip dvmrp report-interval seconds

---

Syntax Definitions

seconds Specifies the report interval, in seconds (10–2000).

---

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> ip dvmrp report-interval 60

Release History

Release 7.1.1; command was introduced.

Related Commands

show ip dvmrp route Displays the DVMRP routes that are being advertised to other routers.

show ip dvmrp Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig
  alaDvmrpRouteReportInterval
ip dvmrp route-holddown

Configures the time during which DVMRP routes are kept in a hold down state. A holddown state refers to the time that a route to an inactive network continues to be advertised.

ip dvmrp route-holddown seconds

__Syntax Definitions__

seconds  Specifies the holddown time, in seconds (1–86400).

__Defaults__

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>120</td>
</tr>
</tbody>
</table>

__Platforms Supported__

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

__Usage Guidelines__

N/A

__Examples__

-> ip dvmrp route-holddown 120

__Release History__

Release 7.1.1; command was introduced.
DVMRP Commands

ip dvmrp route-holddown

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dvmrp route-timeout</td>
<td>Configures the route expiration timeout value.</td>
</tr>
<tr>
<td>show ip dvmrp</td>
<td>Displays the global DVMRP parameters.</td>
</tr>
<tr>
<td>show ip dvmrp route</td>
<td>Displays the DVMRP routes that are being advertised to other routers.</td>
</tr>
</tbody>
</table>

MIB Objects

alaDvmrpGlobalConfig
  alaDvmrpRouteHoldDown
ip dvmrp route-timeout

Configures the route expiration timeout value. The route expiration timeout value specifies how long the switch will wait before aging out a route. When the route expiration timeout expires, the route is advertised as being in holddown until either its activity resumes or it is deleted from the route table.

ip dvmrp route-timeout seconds

Syntax Definitions

seconds Specifies the timeout value, in seconds (20–4000).

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>140</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> ip dvmrp route-timeout 140

Release History

Release 7.1.1; command was introduced.
DVMRP Commands

ip dvmrp route-timeout

Related Commands

- **ip dvmrp route-holddown**  Configures the time during which DVMRP routes are kept in a hold down state.
- **show ip dvmrp**  Displays the global DVMRP parameters.

MIB Objects

- **alaDvmrpGlobalConfig**
  - **alaDvmrpRouteExpirationTimeout**
**ip dvmrp subord-default**

Changes the initial default assumption on a neighbor's subordinate or non-subordinate status. When the status value is true, DVMRP neighbors are assumed to be subordinate and traffic is automatically forwarded to the neighbor upon initial discovery. When the value is false, traffic is not forwarded to the neighbor until route reports have been exchanged and the neighbor has explicitly expressed dependency.

```
ip dvmrp subord-default {true | false}
```

---

**Syntax Definitions**

**true**

DVMRP neighbors are assumed subordinate; traffic is automatically forwarded to the neighbor on initial discovery.

**false**

DVMRP neighbors are *not* assumed to be subordinate; traffic is not forwarded until route reports have been exchanged and the neighbor has explicitly expressed dependency.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>false</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- However, if neighbors in the DVMRP domain have difficulty handling large initial bursts of traffic, it is recommended that the neighbor's default status as a subordinate be changed to false.

- To view the current subordinate neighbor status, use the `show ip dvmrp` command.

---

**Examples**

```
-> ip dvmrp subord-default false
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ip dvmrp
Displays the global DVMRP parameters.

MIB Objects

alaDvmrpGlobalConfig

alaDvmrpInitNbrAsSubord
**show ip dvmrp**

Displays the global DVMRP parameters configuration.

```bash
-> show ip dvmrp
DVMRP Admin Status          = enabled,
Flash Interval              = 5,
Graft Timeout               = 5,
Neighbor Interval           = 10,
Neighbor Timeout            = 35,
Prune Lifetime              = 7200,
Prune Timeout               = 30,
Report Interval             = 60,
Route Holddown              = 120,
Route Timeout               = 140,
Subord Default              = true,
BFD status                  = disabled,
MBR Operational Status      = enabled,
Number of Routes            = 3,
Number of Reachable Routes  = 3
```
### DVMRP Commands

#### show ip dvmrp

**output definitions**

<table>
<thead>
<tr>
<th><strong>DVMRP Admin Status</strong></th>
<th>The current global (i.e., switch-wide) status of DVMRP, which can be <strong>enabled</strong> or <strong>disabled</strong>. To change the current DVMRP global status, use the <strong>ip dvmrp admin-state</strong> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flash Interval</strong></td>
<td>The current minimum flash update interval value, in seconds. The flash interval defines how often routing table change messages are sent to neighboring DVMRP routers. Because routing table change messages are sent between the transmission of complete routing tables, the flash update interval must be shorter than the route report interval. The default value is 5.</td>
</tr>
<tr>
<td><strong>Graft Timeout</strong></td>
<td>The graft message retransmission value, in seconds. The graft message retransmission value defines the duration of time that the routing switch will wait before retransmitting a graft message if it has not received an acknowledgement from its neighbor. Valid range from 5–86400. The default value is 5.</td>
</tr>
<tr>
<td><strong>Neighbor Interval</strong></td>
<td>The current neighbor probe interval time, in seconds. The neighbor probe interval time specifies how often probes are transmitted to interfaces with attached DVMRP neighbors. Valid range from 5–30. The default value is 10.</td>
</tr>
<tr>
<td><strong>Neighbor Timeout</strong></td>
<td>The current neighbor timeout value, in seconds. This value specifies how long the routing switch will wait for activity from a neighboring DVMRP router before assuming the inactive router is down. Valid range from 5–86400. The default value is 35.</td>
</tr>
<tr>
<td><strong>Prune Lifetime</strong></td>
<td>The length of time, in seconds, a prune will be in effect. When the prune lifetime expires, the interface is joined back onto the multicast delivery tree. If unwanted multicast datagrams continue to arrive, the prune mechanism will be re-initiated and the cycle will continue. Valid range from 180–86400. The default value is 7200.</td>
</tr>
<tr>
<td><strong>Prune Timeout</strong></td>
<td>The current prune packet retransmission value, in seconds. This value indicates the duration of time that the routing switch will wait if it continues to receive unwanted multicast traffic before retransmitting a prune message. Valid range from 30–86400. The default value is 30.</td>
</tr>
<tr>
<td><strong>Report Interval</strong></td>
<td>The current route report interval, in seconds. The route report interval defines how often routers will send their complete routing tables to neighboring routers running DVMRP. Valid range from 10–2000. The default value is 60.</td>
</tr>
<tr>
<td><strong>Route Holddown</strong></td>
<td>The current holddown time, in seconds. This value indicates the time during which DVMRP routes are kept in a holddown state. A holddown state refers to the time that a route to an inactive network continues to be advertised. Valid range from 1–120. The default value is 120.</td>
</tr>
<tr>
<td><strong>Route Timeout</strong></td>
<td>The current route expiration timeout value, in seconds. The route expiration timeout value specifies how long the routing switch will wait before aging out a route. Valid range from 20–4000. The default value is 140.</td>
</tr>
</tbody>
</table>


**Release History**

Release 7.1.1; command was introduced.  
Release 7.3.2; **MBR Operational Status** field added.

**Related Commands**

- `ip dvmrp admin-state`  
  Globally enables or disables DVMRP protocol on the switch.

- `ip dvmrp flash-interval`  
  Configures the minimum flash update interval value.

- `ip dvmrp graft-timeout`  
  Configures the graft message retransmission value.

- `ip dvmrp neighbor-timeout`  
  Configures the neighbor timeout.

- `ip dvmrp prune-lifetime`  
  Indicates the length of time a prune will be in effect.

- `ip dvmrp prune-timeout`  
  Configures the prune packet retransmission value.

- `ip dvmrp report-interval`  
  Configures the route report interval.

- `ip dvmrp route-holddown`  
  Configures the time during which DVMRP routes are kept in a hold down state.

- `ip dvmrp route-timeout`  
  Configures the route expiration timeout value.

- `ip dvmrp subord-default`  
  Configures the neighbor probe interval time.
**MIB Objects**

alaDvmrpConfigMIBGroup
  - alaDvmrpAdminStatus
  - alaDvmrpRouteReportInterval
  - alaDvmrpFlashUpdateInterval
  - alaDvmrpNeighborTimeout
  - alaDvmrpRouteExpirationTimeout
  - alaDvmrpRouteHoldDown
  - alaDvmrpNeighborProbeInterval
  - alaDvmrpPruneLifetime
  - alaDvmrpPruneRetransmission
  - alaDvmrpGraftRetransmission
  - alaDvmrpInitNbrAsSubord

dvmrpGeneralGroup
  - dvmrpNumRoutes
  - dvmrpReachableRoutes
**show ip dvmrp interface**

Displays information for all multicast-capable interfaces or for a specified interface. This command also provides options to display only DVMRP-enabled or DVMRP-disabled interfaces.

`show ip dvmrp interface [ip_address | interface_name | enabled | disabled]

---

**Syntax Definitions**

- `ip_address`: Specifies a particular interface IP address.
- `interface_name`: The name of the interface.
- `enabled`: Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently enabled.
- `disabled`: Displays a list of all interfaces (i.e., VLAN router ports) on which DVMRP is currently disabled.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- If no optional syntax is specified in the command line, the entire interface table is displayed.
- For an interface to show as `enabled` in the `show ip dvmrp interface` or `show ip dvmrp interface enabled` output, the interface must be both administratively and operationally enabled. Although the interface does not have to be passing traffic, at least one VLAN router port must be operational on the corresponding DVMRP-enabled VLAN.
- To view the Generation ID being used on a particular interface, you must include the interface IP address in the command line.

**Examples**

```
-> show ip dvmrp interface

Total 4 Interfaces

Interface Name  Vlan  Metric  Admin-Status  Oper-Status  BFD-Status  MBR-Default
-----------------+-----+------+--------------+-------------+----------+-----------
 vlan-4 4 1  Disabled  Disabled  Disabled  Disabled
```
DVMRP Commands

show ip dvmrp interface

```
  vlan-6  6  1  Enabled  Enabled  Disabled  Enabled
```

-> show ip dvmrp interface enabled

Total 1 Interfaces

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Vlan</th>
<th>Metric</th>
<th>Admin-Status</th>
<th>Oper-Status</th>
<th>BFD-Status</th>
<th>MBR-Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-6</td>
<td>6</td>
<td>1</td>
<td>Enabled</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>The name of the interface.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The associated VLAN ID.</td>
</tr>
<tr>
<td>Tunnel</td>
<td>Indicates whether there is a DVMRP tunnel currently configured on the interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.</td>
</tr>
<tr>
<td>Admin-Status</td>
<td>The current administrative status of the corresponding interface. Options include Enabled or Disabled. An interface can be configured for DVMRP without being operational. To change the DVMRP Admin-status for an individual interface, refer to the ip dvmrp interface command.</td>
</tr>
<tr>
<td>Oper-Status</td>
<td>The current operational status of the corresponding multicast-capable interface. Options include Enabled or Disabled. For an interface to be DVMRP-operational, the global DVMRP status must be enabled and the individual interface must be DVMRP-enabled. To change the global DVMRP status, refer to the ip dvmrp admin-state command.</td>
</tr>
<tr>
<td>BFD-Status</td>
<td>Not supported in the current release.</td>
</tr>
<tr>
<td>MBR-Default</td>
<td>Whether or not the DVMRP interface will advertise a default route when the interface is configured on a Multicast Border Router. Options include Enabled or Disabled. Configured through the ip dvmrp interface mbr-default-information command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.2; **MBR-Default** field added.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dvmrp interface</td>
<td>Enables or disables the DVMRP protocol on a specified interface.</td>
</tr>
</tbody>
</table>

**MIB Objects**

dvmrpInterfaceGroup
  dvmarpInterfaceLocalAddress
  dvmarpInterfaceMetric
  dvmarpInterfaceStatus
DVMRP Commands

show ip dvmrp interface

alaDvmrpIfAugTable
  alaDvmrpIfMbrDefaultInfoStatus
**show ip dvmrp neighbor**

Displays the DVMRP neighbor table. The DVMRP neighbor table displays either all neighboring DVMRP routers, or a specified neighboring DVMRP router.

**Syntax**

```
show ip dvmrp neighbor [ip_address]
```

**Syntax Definitions**

*ip_address*    Specifies a particular IP address for a neighboring DVMRP router.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If a neighbor IP address is not specified, the entire DVMRP Neighbor Table is displayed.

**Examples**

```
-> show ip dvmrp neighbor
```

```
Neighbor Address   Intf Name     Uptime      Expires     GenID     Vers  State
----------------+-------------+-----------+-----------+----------+------+-------
143.209.92.214 vlan-2 00h:09m:12s 00h:00m:06s 546947509 3.255 active
```

**output definitions**

- **Neighbor Address**: The 32-bit IP address of the DVMRP neighbor’s router interface.
- **Intf Name**: The interface name of the neighbor’s router.
- **Uptime**: The amount of time the neighbor has been running, displayed in hours, minutes, and seconds.
- **Expires**: The amount of time remaining before the neighbor expires, displayed in hours, minutes, and seconds.
- **GenID**: The generation ID for the DVMRP neighbor. This value is used by neighboring routers to detect whether the DVMRP routing table should be resent.
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The DVMRP version number for the neighbor.</td>
</tr>
<tr>
<td>State</td>
<td>The current state of the DVMRP neighbor. Options include active and down.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip dvmrp neighbor-interval` Configures the neighbor probe interval time.
- `ip dvmrp neighbor-timeout` Configures the neighbor timeout.

**MIB Objects**

dvmrpNeighborTable
  - dvmrpNeighborAddress
  - dvmrpNeighborIfIndex
  - dvmrpNeighborUpTime
  - dvmrpNeighborExpiryTime
  - dvmrpNeighborGenerationId
  - dvmrpNeighborMajorVersion
  - dvmrpNeighborMinorVersion
  - dvmrpNeighborState
show ip dvmrp nexthop

Displays DVMRP next hop entries. This command is used to show the list of next hops on outgoing interfaces to which IP multicast datagrams from particular sources are routed.

**Syntax Definitions**

| ip_address | Specifies a source IP address for which DVMRP next hop entries will be displayed. |
| ip_mask    | Specifies a source IP mask for which DVMRP next hop entries will be displayed. |

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If an IP address and IP mask are not specified, the entire DVMRP Next Hop table is displayed.

**Examples**

```
-> show ip dvmrp nexthop 172.22.2.115 255.255.255.0
```

<table>
<thead>
<tr>
<th>Src Address/Mask</th>
<th>Interface Name</th>
<th>Vlan</th>
<th>Hop Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.22.2.115/24</td>
<td>vlan-2</td>
<td>2</td>
<td>branch</td>
</tr>
</tbody>
</table>

**output definitions**

- **Src Address/Mask**: The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
- **Interface Name**: The name of the interface.
- **Vlan**: The associated VLAN ID.
- **Hop Type**: The hop type of the associated entry. Options include leaf or branch. If the next hop VLAN has a DVMRP neighbor attached to it, the hop type will be displayed as branch.
Release History

Release 7.1.1; command was introduced.

Related Commands

N/A

MIB Objects

dvmrpRouteNextHopTable
  dvmrpRouteNextHopSource
  dvmrpRouteNextHopSourceMask
  dvmrpRouteNextHopIfIndex
  dvmrpRouteNextHopType
show ip dvmrp prune

Displays DVMRP prune entries that have been sent upstream.

**show ip dvmrp prune [group_address source_address source_mask]**

---

### Syntax Definitions

- **group_address**: Specifies a pruned group address.
- **source_address**: Specifies a source IP address.
- **source_mask**: Specifies a source IP mask.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If a group address, source address, and source mask are not specified, the entire Prune table is displayed.

### Examples

```
-> show ip dvmrp prune
```

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address/Mask</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.0.4</td>
<td>143.209.92.14/24</td>
<td>00h:00m:30s</td>
</tr>
</tbody>
</table>

**output definitions**

- **Group Address**: The 32-bit multicast group address.
- **Source Address/Mask**: The 32-bit source IP address, along with the mask length, shown in bits. The source IP address and mask are separated by a slash (/).
- **Expires**: The amount of time remaining before the current prune state expires, displayed in hours, minutes, and seconds.

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ip dvmrp prune-lifetime` Indicates the length of time a prune will be in effect.
- `ip dvmrp prune-timeout` Configures the prune packet retransmission value.

**MIB Objects**

dvmrpPruneTable
  
dvmrpPruneGroup
dvmrpPruneSource
dvmrpPruneSourceMask
dvmrpPruneExpiryTime
show ip dvmrp route

Displays the DVMRP routes that are being advertised to other routers.

show ip dvmrp route [ip_address ip_mask]

Syntax Definitions

ip_address The 32-bit source IP address representing route(s).
ip_mask A 32-bit number that determines the subnet mask for the IP address.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 C32E/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

If a source IP address and IP mask are not specified, the entire DVMRP route table is displayed.

Examples

-> show ip dvmrp route

Legends: Flags: L = Local, R = Remote, F = Flash, H = Holddown, I = Invalid

<table>
<thead>
<tr>
<th>Address/Mask</th>
<th>Gateway</th>
<th>Metric</th>
<th>Age</th>
<th>Expires</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0.0.0/8</td>
<td>55.0.0.5</td>
<td>2</td>
<td>00h:13m:14s</td>
<td>02m:07s</td>
<td>R</td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>44.0.0.4</td>
<td>2</td>
<td>00h:33m:14s</td>
<td>02m:15s</td>
<td>R</td>
</tr>
<tr>
<td>44.0.0.0/8</td>
<td>-</td>
<td>1</td>
<td>05h:24m:59s</td>
<td>-</td>
<td>L</td>
</tr>
<tr>
<td>55.0.0.0/8</td>
<td>-</td>
<td>1</td>
<td>05h:24m:59s</td>
<td>-</td>
<td>L</td>
</tr>
<tr>
<td>66.0.0.0/8</td>
<td>44.0.0.4</td>
<td>2</td>
<td>00h:03m:11s</td>
<td>02m:15s</td>
<td>R</td>
</tr>
</tbody>
</table>

output definitions

Address/Mask The 32-bit IP address for the router interface, along with the corresponding subnet mask. The interface’s subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals /16; 255.255.255.0 equals /24, etc.

Gateway The corresponding 32-bit gateway address. Because it is not applicable, no gateway address is displayed for local routes.
output definitions (continued)

<table>
<thead>
<tr>
<th>Metric</th>
<th>The current metric value. A metric is essentially used to determine the most cost-effective way to pass data through the network. The higher the metric value, the higher the cost.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>The current age of the DVMRP route, displayed in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Expires</td>
<td>The expiration time for the corresponding route. Because it is not applicable, no expiration time is displayed for local routes.</td>
</tr>
<tr>
<td>Flags</td>
<td>The flag type of a particular DVMRP route. Options include L (Local), R (Remote), F (Flash), H (Holddown), and I (Invalid).</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip dvmrp report-interval` Configures the route report interval.
- `ip dvmrp route-holdown` Configures the time during which DVMRP routes are kept in a hold down state.
- `ip dvmrp route-timeout` Configures the route expiration timeout value.

**MIB Objects**

- `dvmrpRouteTable`
- `dvmrpRouteSource`
- `dvmrpRouteSourceMask`
- `dvmrpRouteMetric`
- `dvmrpRouteExpiryTime`
- `dvmrpRouteUpTime`
show ip dvmrp tunnel

Displays DVMRP tunnel entries.

show ip dvmrp tunnel [local_address remote_address]

Syntax Definitions

| local_address | The IP address of a particular local router interface. The local router interface IP address is an identifier for the local end of the DVMRP tunnel. |
| remote_mask | The IP address of a particular remote router interface. The remote router interface IP address is an identifier for the remote end of the DVMRP tunnel. |

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- If optional local and remote IP address information is not specified, entire DVMRP Tunnels table is displayed.
- The local IP address of the tunnel must match the IP address of an existing DVMRP-enabled IP interface.

Examples

-> show ip dvmrp tunnel

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Local Address</th>
<th>Remote Address</th>
<th>TTL</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-2</td>
<td>143.209.92.203</td>
<td>12.0.0.1</td>
<td>255</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

output definitions

- Interface Name: The interface name.
- Local Address: The 32-bit local IP address for the DVMRP tunnel.
- Remote Address: The 32-bit remote IP address for the DVMRP tunnel.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTL</td>
<td>The current Time to Live (TTL) value. A value of 0 indicates that the value is copied from the payload’s header. Valid range from 0–255.</td>
</tr>
<tr>
<td>Status</td>
<td>The corresponding interface status. Options include Enabled or Disabled. If the interface specified by the local address has been configured and is operationally enabled, the status is Enabled. If the interface is down, the value displayed is Disabled.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip interface tunnel` Adds or deletes a DVMRP tunnel.
- `show ip dvmrp` Configures the TTL value for the tunnel defined for the specified local address and remote address.

**MIB Objects**

- `tunnelIfTable`
  - `tunnelIfLocalAddress`
  - `tunnelIfRemoteAddress`
  - `tunnelIfHopLimit`
- `dvmrpInterfaceGroup`
  - `dvmrpInterfaceStatus`
Protocol-Independent Multicast (PIM) is an IP multicast routing protocol that uses routing information provided by unicast routing protocols, such as RIP and OSPF. Note that PIM is not dependent on any particular unicast routing protocol. Sparse mode PIM (PIM-SM) contrasts with flood-and-prune dense mode multicast protocols, such as DVMRP and PIM Dense Mode (PIM-DM), in that multicast forwarding in PIM-SM is initiated only through specific requests.

Downstream routers must explicitly join PIM-SM distribution trees to receive multicast streams on behalf of directly connected receivers or other downstream PIM-SM routers. This paradigm of receiver-initiated forwarding makes PIM ideal for network environments where receiver groups are thinly populated and bandwidth conservation is a concern, such as in wide area networks (WANs).

PIM-SIM builds unidirectional shared trees that are rooted at a Rendezvous Point (RP) multicast router. Bidirectional PIM (BIDIR-PIM) is a variant of PIM-SM that builds bidirectional shared trees also rooted at an RP. However, BIDIR-PIM forwards packets from the source to the RP without the overhead of encapsulation or source-specific states.

PIM-DM uses RPF (Reverse Path Forwarding) to prevent looping of multicast datagrams while flooding. If some areas of the network do not have group members, PIM-DM will prune the forwarding branch by instantiating the prune state.

PIM-DM differs from PIM-SM in two essential ways:

- There are no periodic joins transmitted, only explicitly triggered prunes and grafts.
- There is no Rendezvous Point (RP). This is particularly important in networks that cannot tolerate a single point of failure.

The OmniSwitch implementation of PIM can also be configured in an IPv6 environment.

MIB information for the PIM commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-VIRTUALROUTER-MIB.mib</td>
<td>alcatelIND1VirtualRouterMIB</td>
</tr>
<tr>
<td>ALCATEL-IND1-PIM-MIB.mib</td>
<td>alcatelIND1PIMMIB</td>
</tr>
<tr>
<td>PIM-BSR-MIB.mib</td>
<td>pimBsrMIB</td>
</tr>
<tr>
<td>PIM-STD-MIB.mib</td>
<td>pimStdMIB</td>
</tr>
</tbody>
</table>
A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>Command</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip load pim</td>
<td>show ip pim static-rp</td>
</tr>
<tr>
<td>ip pim sparse admin-state</td>
<td>show ip pim anycast-rp</td>
</tr>
<tr>
<td>ip pim bidir admin-state</td>
<td>show ip pim cbsr</td>
</tr>
<tr>
<td>ip pim dense admin-state</td>
<td>show ip pim bsr</td>
</tr>
<tr>
<td>ip pim rp-hash admin-state</td>
<td>show ip pim notifications</td>
</tr>
<tr>
<td>ip pim ssm group</td>
<td>show ip pim groute</td>
</tr>
<tr>
<td>ip pim dense group</td>
<td>show ip pim sgroute</td>
</tr>
<tr>
<td>ip pim cbsr</td>
<td>show ip pim df-election</td>
</tr>
<tr>
<td>ip pim static-rp</td>
<td>ipv6 pim sparse admin-state</td>
</tr>
<tr>
<td>ip pim anycast-rp</td>
<td>ipv6 pim bidir admin-state</td>
</tr>
<tr>
<td>ip pim candidate-rp</td>
<td>ipv6 pim dense admin-state</td>
</tr>
<tr>
<td>ip pim rp-threshold</td>
<td>ipv6 pim ssm group</td>
</tr>
<tr>
<td>ip pim keepalive-period</td>
<td>ipv6 pim dense group</td>
</tr>
<tr>
<td>ip pim max-rps</td>
<td>ipv6 pim cbsr</td>
</tr>
<tr>
<td>ip pim probe-time</td>
<td>ipv6 pim static-rp</td>
</tr>
<tr>
<td>ip pim register checksum</td>
<td>ipv6 pim anycast-rp</td>
</tr>
<tr>
<td>ip pim register-packing</td>
<td>ipv6 pim candidate-rp</td>
</tr>
<tr>
<td>ip pim register-mtu</td>
<td>ipv6 pim rp-switchover</td>
</tr>
<tr>
<td>ip pim register-delay</td>
<td>ipv6 pim register-rate-limit</td>
</tr>
<tr>
<td>ip pim register-suppress-timeout</td>
<td>ipv6 pim register-packing</td>
</tr>
<tr>
<td>ip pim register-rate-limit</td>
<td>ipv6 pim register-mtu</td>
</tr>
<tr>
<td>ip pim spt admin-state</td>
<td>ipv6 pim register-delay</td>
</tr>
<tr>
<td>ip pim state-refresh-interval</td>
<td>ipv6 pim spt admin-state</td>
</tr>
<tr>
<td>ip pim state-refresh-limit</td>
<td>ipv6 pim interface</td>
</tr>
<tr>
<td>ip pim state-refresh-ttl</td>
<td>ipv6 pim bfd-state</td>
</tr>
<tr>
<td>ip pim interface</td>
<td>ipv6 pim bfd-state all-interfaces</td>
</tr>
<tr>
<td>ip pim neighbor-loss-notification-period</td>
<td>ipv6 pim interface bfd-state</td>
</tr>
<tr>
<td>ip pim invalid-register-notification-period</td>
<td>ipv6 pim bidir ssm-compat</td>
</tr>
<tr>
<td>ip pim invalid-joinprune-notification-period</td>
<td>ipv6 pim bidir fast-join</td>
</tr>
<tr>
<td>ip pim rp-mapping-notification-period</td>
<td>ipv6 pim sparse asm-fast-join</td>
</tr>
<tr>
<td>ip pim interface-election-notification-period</td>
<td>ipv6 pim sparse ssm-fast-join</td>
</tr>
<tr>
<td>ip pim nonbidir-hello-notification-period</td>
<td>ipv6 pim joinprune-packing</td>
</tr>
<tr>
<td>ip pim df-abort</td>
<td>show ipv6 pim sparse</td>
</tr>
<tr>
<td>ip pim mbr all-sources</td>
<td>show ipv6 pim dense</td>
</tr>
<tr>
<td>ip pim df-periodic-interval</td>
<td>show ipv6 pim ssm group</td>
</tr>
<tr>
<td>ip pim bfd-state</td>
<td>show ipv6 pim dense group</td>
</tr>
<tr>
<td>ip pim bfd-state all-interfaces</td>
<td>show ipv6 pim interface</td>
</tr>
<tr>
<td>ip pim interface bfd-state</td>
<td>show ipv6 pim bfd-state all-interfaces</td>
</tr>
<tr>
<td>ip pim bidir ssm-compat</td>
<td>show ipv6 pim neighbor</td>
</tr>
<tr>
<td>ip pim bidir fast-join</td>
<td>show ipv6 pim static-rp</td>
</tr>
<tr>
<td>ip pim sparse asm-fast-join</td>
<td>show ipv6 pim anycast-rp</td>
</tr>
<tr>
<td>ip pim sparse ssm-fast-join</td>
<td>show ipv6 pim group-map</td>
</tr>
<tr>
<td>ip pim joinprune-packing</td>
<td>show ipv6 pim candidate-rp</td>
</tr>
<tr>
<td>show ip pim sparse</td>
<td>show ipv6 pim cbsr</td>
</tr>
<tr>
<td>show ip pim dense</td>
<td>show ipv6 pim bsr</td>
</tr>
<tr>
<td>show ip pim ssm group</td>
<td>show ipv6 pim groute</td>
</tr>
<tr>
<td>show ip pim dense group</td>
<td>show ipv6 pim sgroute</td>
</tr>
<tr>
<td>show ip pim neighbor</td>
<td>show ipv6 pim df-election</td>
</tr>
<tr>
<td>show ip pim candidate-rp</td>
<td></td>
</tr>
<tr>
<td>show ip pim group-map</td>
<td></td>
</tr>
<tr>
<td>show ip pim interface</td>
<td></td>
</tr>
</tbody>
</table>
**ip load pim**

Dynamically loads PIM to memory.

**ip load pim**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command must be executed before PIM can run on the switch.
- This command is supported in both IPv4 and IPv6 PIM.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

**Examples**

-> ip load pim

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip pim sparse admin-state**: Globally enables or disables the PIM-SM protocol on the switch.
- **ip pim bidir admin-state**: Globally enables or disables the BIDIR-PIM protocol on the switch.
- **show ip pim sparse**: Displays the status of the various global parameters for the PIM sparse mode.
- **ip pim dense admin-state**: Globally enables or disables PIM-DM protocol on the switch.
- **show ip pim dense**: Displays the status of the various global parameters for the PIM Dense mode.
- **ipv6 pim sparse admin-state**: Enables or disables IPv6 PIM-SM (sparse mode) globally for IPv6.
- **ipv6 pim bidir admin-state**: Enables or disables IPv6 BIDIR-PIM (bidirectional) globally for IPv6.
- **show ipv6 pim sparse**: Displays the status of the various global parameters for the IPv6 PIM sparse mode.
- **ipv6 pim dense admin-state**: Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.
- **show ipv6 pim dense**: Displays the status of the various global parameters for the IPv6 PIM dense mode.

MIB Objects

- **alaVrConfigTable**
  - **alaVrConfigPimStatus**
ip pim sparse admin-state

Globally enables or disables PIM-SM protocol on the switch.

`ip pim sparse admin-state {enable | disable}`

### Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Globally enables PIM-SM on the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Globally disables PIM-SM on the switch.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command must be set to `enable` before PIM-SM can run on the switch. In addition, the `ip load pim` command must be executed. Refer to page 34-3 for more information.
- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

### Examples

```
-> ip pim sparse admin-state enable
-> ip pim sparse admin-state disable
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **ip pim interface**
  Enables or disables the PIM protocol on a specific interface.
- **ip load pim**
  Dynamically loads PIM to memory.
- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

- **alaPimsmGlobalConfig**
  - **alaPimsmAdminStatus**
ip pim bidir admin-state

Globally enables or disables the BIDIR-PIM protocol on the switch.

ip pim bidir admin-state {enable | disable}

----

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Globally enables BIDIR-PIM on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Globally disables BIDIR-PIM on the switch.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command must be set to **enable** before BIDIR-PIM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 34-3 for more information.

- BIDIR-PIM is a variant of PIM-SM, which means that PIM-SM must also be globally enabled on the switch.

**Examples**

-> ip pim bidir admin-state enable

-> ip pim bidir admin-state disable

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- **ip pim interface**: Enables or disables the PIM protocol on a specific interface.
- **ip load pim**: Dynamically loads PIM to memory.
- **show ip pim sparse**: Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

- alaPimsmGlobalConfig
- alaPimsmBidirStatus
**ip pim dense admin-state**

Globally enables or disables PIM-DM protocol on the switch.

`ip pim dense admin-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Globally enables PIM-DM on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Globally disables PIM-DM on the switch.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command must be set to `enable` before PIM-DM can run on the switch. In addition, the `ip load pim` command must be executed. Refer to page 34-3 for more information.

- The advanced routing image file must be loaded to flash before the feature will start to work on the switch.

**Examples**

- `-> ip pim dense admin-state enable`
- `-> ip pim dense admin-state disable`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ip pim interface**
  Enables or disables the PIM protocol on a specific interface.

- **ip load pim**
  Dynamically loads PIM to memory.

- **show ip pim dense**
  Displays the status of the various global parameters for the PIM dense mode.

**MIB Objects**

- **alaPimdmGlobalConfig**
- **alaPimdmAdminStatus**
**ip pim rp-hash admin-state**

Configures the version of the hashing algorithm that the Rendezvous Point (RP) hashing function will use to select an RP.

```
ip pim rp-hash admin-state {enable | disable}
```

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Applies the newer version of the hashing algorithm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Applies the legacy version of the hashing algorithm.</td>
</tr>
</tbody>
</table>

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The RP hashing function is applied when selecting an RP from two or more equal group-range-to-RP mappings.

- To maintain interoperability between PIM routers, make sure all routers have the same setting for the RP hash function. For example, this function is enabled for all PIM routers or this function is disabled for all PIM routers.

---

**Examples**

```
-> ip pim rp-hash admin-state enable
-> ip pim rp-hash admin-state disable
```

---

**Release History**

Release 7.3.4; command was introduced.
**Related Commands**

*show ip pim sparse* Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

alaPimsmGlobalConfig
alaPimsmRPHashStatus


**ip pim ssm group**

Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).

```
ip pim ssm group group_address/prefix_length [no] override [priority priority]
no ip pim ssm group group_address/prefix_length
```

### Syntax Definitions

- **group_address** Specifies a 32-bit group address.
- **/prefix_length** Specifies the prefix length of the multicast group.
- **override** Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
- **priority** Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

### Defaults

By default, the priority option is not set and the override option is set to false.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove a static configuration of a SSM mode group mapping.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and needs to be configured manually to support SSM.
- You can also map additional multicast address ranges for the SSM group using this command. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the `override` option.
- Note that once the priority option has been defined, a value of 65535 can be used to unset the priority.
**Examples**

`-> ip pim ssm group 225.0.0.0/24 priority 50`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip pim sparse`: Displays the status of the various global parameters for the PIM sparse mode.
- `show ip pim ssm group`: Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.
- `show ip pim group-map`: Displays the PIM group mapping table.

**MIB Objects**

- `pimStaticRPTable`:
  - `pimStaticRPGrpAddress`
  - `pimStaticRPGrpPrefixLength`
  - `pimStaticRPImMode`
  - `pimStaticRPPrecedence`
  - `pimStaticRPOverrideDynamic`
  - `pimStaticRPRowStatus`
**ip pim dense group**

Statically maps the specified IP multicast group(s) to the PIM Dense mode (DM).

```
ip pim dense group group_address/prefix_length [no] override [priority priority]
```

```
no ip pim dense group group_address/prefix_length
```

**Syntax Definitions**

- **group_address**
  Specifies a 32-bit group address.

- **/prefix_length**
  Specifies the prefix length of the multicast group.

- **override**
  Specifies that this static Dense mode mapping configuration should override the dynamically learned group mapping information for the specified group(s).

- **priority**
  Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

**Defaults**

By default, the priority option is not set and the override option is set to false.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified multicast group address.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the **override** option and once the priority option has been defined, a value of 65535 can be used to unset the priority.

**Examples**

```
-> ip pim dense group 225.0.0.0/24 priority 50
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip pim dense` Displays the status of the various global parameters for the PIM dense mode.
- `show ip pim dense group` Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).
- `show ip pim group-map` Displays the PIM group mapping table.

**MIB Objects**

- `alaPimdmDenseGroupTable`  
  - `alaPimdmDenseGroupGrpAddress`
  - `alaPimdmDenseGroupGrpPrefixLength`
  - `alaPimdmDenseGroupOverrideDynamic`
  - `alaPimdmDenseGroupPrecedence`
  - `alaPimdmDenseGroupRowStatus`
**ip pim cbsr**

Configures the local router as the Candidate-BSR for the PIM domain.

```
ip pim cbsr ip_address [priority priority] [mask-length bits]
```

```
o ip pim cbsr ip_address
```

---

**Syntax Definitions**

- **ip_address** Specifies the 32-bit address that the local router uses to advertise itself as a Candidate-BSR.
- **priority** Specifies the priority value of the local router as a Candidate-BSR. The higher the value, the higher the priority. Values may range from 0–255.
- **bits** Specifies a 32-bit mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group). Values may range from 1–32.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>64</td>
</tr>
<tr>
<td>bits</td>
<td>30</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to remove the local routers candidature as the BSR.
- This command is supported only in the sparse mode.
- The information configured using this command is used in the Bootstrap messages.
- Candidate-BSRs also avoid a single point of failure in a PIM domain.

---

**Examples**

```
-> ip pim cbsr 50.1.1.1 priority 100 mask-length 4
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ip pim cbsr` Displays the Candidate-BSR information that is used in the Bootstrap messages.

**MIB Objects**

- `pimBsrCandidateBSRTable`
  - `pimBsrCandidateBSRAAddress`
  - `pimBsrCandidateBSRPriority`
  - `pimBsrCandidateBSRHashMaskLength`
  - `pimBsrCandidateBSRRowStatus`
**ip pim static-rp**

Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

```
ip pim static-rp group_address/prefix_length rp_address [[no] bidir] [[no] override] [priority priority]
no ip pim static-rp group_address/prefix_length rp_address
```

### Syntax Definitions

- `group_address`  
  Specifies a 32-bit group address.
- `/prefix_length`  
  Specifies the prefix length of the multicast group.
- `rp_address`  
  Specifies a 32-bit Rendezvous Point (RP) address.
- `bidir`  
  Creates the static RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.
- `override`  
  Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
- `priority`  
  Specifies the preference value to be used for the static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

### Defaults

By default, the `priority` option is not set, the `override` option is set to false, and the `bidir` option is set to false.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the `override` option.
- If the `bidir` parameter option is not specified with this command, the static RP entry is created for use in the ASM mode.
- The PIM Source-Specific Multicast (SSM) mode for the default SSM address range (232.0.0.0 through 232.255.255.255) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM. You can also map additional multicast address
ranges for the SSM group. However, the multicast groups in the reserved address range can be mapped only to the SSM mode.

- This command is supported only in the sparse mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Note that once the priority option has been defined, a value of 65535 can be used to unset the priority.
- To view current static RP configuration settings, use the `show ip pim static-rp` command.

**Examples**

- `-> ip pim static-rp 225.0.0.0/24 10.1.1.1 priority 10`
- `-> ip pim static-rp 225.0.0.0/24 10.1.1.1 bidir override`
- `-> no ip pim static-rp 225.0.0.0/24 10.1.1.1`

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; `bidir` parameter added.

**Related Commands**

- `show ip pim sparse` Displays the status of the various global parameters for the PIM sparse mode.
- `show ip pim static-rp` Displays the PIM static RP table for ASM mode, which includes the group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the static RP configuration (i.e., enabled or disabled).
- `show ip pim group-map` Displays the PIM group mapping table.

**MIB Objects**

- `pimStaticRPTable`
  - `pimStaticRPGrpAddress`
  - `pimStaticRPGrpPrefixLength`
  - `pimStaticRPGrpAddress`
  - `pimStaticRPGrpPrefixLength`
  - `pimStaticRPGrpMode`
  - `pimStaticRPGrpOverrideDynamic`
  - `pimStaticRPGrpPrecedence`
  - `pimStaticRPGrpRowStatus`
**ip pim anycast-rp**

Configures the anycast RP set, which is the set of all routers that would act as the RP.

```plaintext
ip pim anycast-rp anycast_rp_address rp_address
no ip pim anycast-rp anycast_rp_address rp_address
```

### Syntax Definitions

- **anycast-rp-address**: Specifies the anycast RP address.
- **rp_address**: Specifies a 32-bit Rendezvous Point (RP) address of a router that is a member of the anycast RP set.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the no form of this command to delete an anycast RP configuration.
- The RP specified by anycast-RP-address is the RP in the anycast RP set. This address must be the same as the RP address in the Static-RP configuration used with the `ip pim static-rp` command if static RP configuration is being used.
- It is recommended not to use Loopback0 as the anycast RP address since Loopback0 is often used as the Router ID by default with the unicast routing protocols. Hence, it is recommended to use one of the additional LoopbackX interfaces for the anycast RP address, but it is not mandatory to be a LoopbackX address.
- The RP specified by rp-address defines the IP address of the prospective RP. This address must be different than the anycast RP address and is used in communication between the different RPs in the anycast RP set. This configuration must be the same on all routers in the Anycast-RP set.
- There must be a separate entry for each of the RPs participating in anycast RP set, including an entry for the local router. This configuration defining the anycast RP set must be the same on all routers participating in anycast RP.
- It is recommended to configure PIM register rate limiting (see `ip pim register-rate-limit`) to limit the sending of PIM register messages with Anycast RP.
- Ensure SPT is enabled (see `ip pim spt admin-state`) when using Anycast RP. If SPT is globally disabled, and Anycast RP configuration is added, this configuration will be ignored for all groups that are operating in Anycast-RP mode.

**Examples**

- `-> ip pim static-rp 224.0.0.0/4 10.10.10.1`  
- `-> ip pim anycast-rp 10.10.10.1 10.1.1.1`  
- `-> ip pim anycast-rp 10.10.10.1 10.1.1.2`  
- `-> no ip pim anycast-rp 10.10.10.1 10.1.1.2`

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

- `ip pim static-rp`  
  Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

- `show ip pim anycast-rp`  
  Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration

**MIB Objects**

- `pimAnycastRPSetTable`
  - `pimAnycastRPSetAddressType`
  - `pimAnycastRPSetAddress`
  - `pimAnycastRPSetRouterAddress`
  - `pimAnycastRPSetRowStatus`
**ip pim candidate-rp**

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

```
ip pim candidate-rp rp_address group-address/prefix_length [no] bidir [priority priority] [interval seconds]
```

```
o ip pim candidate-rp rp_address group-address/prefix_length
```

**Syntax Definitions**

- `rp_address` Specifies a 32-bit address that will be advertised as a Candidate-RP.
- `group_address` Specifies a 32-bit group address for which the local router will advertise itself as a Candidate-RP.
- `/prefix_length` Specifies the prefix length of the multicast group.
- `bidir` Creates a C-RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.
- `priority` Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.
- `seconds` Specifies the interval at which the C-RP advertisements are sent to the bootstrap router, in seconds. Values may range from 1 to 300.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] bidir</td>
<td>no bidir</td>
</tr>
<tr>
<td>priority</td>
<td>192</td>
</tr>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the association of the device as a C-RP for a particular multicast group.
- The specified `rp_address` must belong to a PIM enabled interface.
Only one RP address is supported per switch. If multiple C-RP entries are defined, they must specify the same rp-address.

If the bidir parameter option is not specified with this command, the C-RP entry is created for use in the ASM mode.

The priority and the interval values are used by the switch. If they are modified for one entry, the switch will modify these for all the C-RP entries.

This command is supported only in the sparse mode.

**Examples**

```
-> ip pim candidate-rp 50.1.1.1 225.0.0.0/24 priority 100 interval 100
-> ip pim candidate-rp 50.1.1.1 225.0.0.0/24 bidir priority 100 interval 100
-> no ip pim candidate-rp 50.1.1.1 225.0.0.0/24
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; bidir parameter added.

**Related Commands**

- `show ip pim candidate-rp`: Displays the IP multicast groups for which the local router will advertise itself as a Candidate-RP.

**MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>pimBsrCandidateRPTable</td>
</tr>
<tr>
<td>pimBsrCandidateRPAddress</td>
</tr>
<tr>
<td>pimBsrCandidateRPGroupAddress</td>
</tr>
<tr>
<td>pimBsrCandidateRPGroupPrefixLength</td>
</tr>
<tr>
<td>pimBsrCandidateRPBidir</td>
</tr>
<tr>
<td>pimBsrCandidateRPPriority</td>
</tr>
<tr>
<td>pimBsrCandidateRPAAdvInterval</td>
</tr>
<tr>
<td>pimBsrCandidateRPRowStatus</td>
</tr>
</tbody>
</table>
**ip pim rp-threshold**

Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a source-specific (S, G) Join message toward the source.

**ip pim rp-threshold** *bps*

---

**Syntax Definitions**

*bps* The data rate value, in bits per second, at which the RP will attempt to switch to native forwarding (0–2147483647).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>bps</em></td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command is supported only in the sparse mode.
- To disable the RP threshold feature, specify a bits per second value of 0. When the RP threshold is disabled, the RP will never initiate an (S, G) Join message toward the source; the packets will be register-encapsulated to the RP. It will issue a (S, G) Join message upon receiving the first data packet, if its bits per second value is 1.
- To view the current RP threshold, use the `show ip pim sparse` command.

---

**Examples**

```
-> ip pim rp-threshold 131072
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ip pim sparse

Displays the global parameters for PIM sparse mode.

MIB Objects

alaPimsmGlobalConfig

alaPimsmRPThreshold
ip pim keepalive-period

Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.

```
ip pim keepalive-period seconds
```

**Syntax Definitions**

seconds Specifies the timeout value, in seconds (0-65535).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>210</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This timer is called the Keepalive Period in the PIM-SM specification and the Source Lifetime in the PIM-DM specification.

- This command includes support for both IPv4 PIM and IPv6 PIM.

**Examples**

```
-> ip pim keepalive-period 500
```

**Release History**

Release 7.1.1; command was introduced.
## Related Commands

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

- **show ip pim dense**
  Displays the status of the various global parameters for the PIM dense mode.

- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

- **show ipv6 pim dense**
  Displays the status of the various global parameters for the IPv6 PIM dense mode.

## MIB Objects

- **pim**
  - **pimKeepalivePeriod**
**ip pim max-rps**

Configures the maximum number of C-RP routers allowed in the PIM-SM domain.

**ip pim max-rps number**

---

**Syntax Definitions**

`number` The maximum number of C-RP routers allowed in the PIM-SM domain (1–100).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>32</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

---

**Usage Guidelines**

- This command is supported only in the sparse mode.
- This command is used with both IPv4 and IPv6 PIM-SM. The PIM-SM must be disabled before changing `max-rps` value.
- PIM-SM must be globally disabled before changing the maximum number of C-RP routers. To globally disable PIM-SM, refer to the `ip pim sparse admin-state` command on page 34-5.

---

**Examples**

```bash
-> ip pim max-rps 32
```

---

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ip pim sparse admin-state**
  Globally enables or disables the PIM-SM protocol on the switch.

- **ipv6 pim sparse admin-state**
  Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

**MIB Objects**

- **alaPimsmGlobalConfig**
- **alaPimsmMaxRPs**
**ip pim probe-time**

Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.

**ip pim probe-time seconds**

---

### Syntax Definitions

seconds | The probe time, in seconds (1–300).

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>5</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is used with both IPv4 and IPv6 PIM-SM.
- This command is supported only in the sparse mode.

### Examples

```
-> ip pim probe-time 5
```

### Release History

Release 7.1.1; command was introduced.
**PIM Commands**

**ip pim probe-time**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show ip pim sparse</strong></td>
<td>Displays the status of the various global parameters for the PIM sparse mode.</td>
</tr>
<tr>
<td><strong>show ipv6 pim sparse</strong></td>
<td>Displays the status of the various global parameters for the IPv6 PIM sparse mode.</td>
</tr>
</tbody>
</table>

**MIB Objects**

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaPimsmGlobalConfig</td>
<td></td>
</tr>
<tr>
<td>alaPimsmProbeTime</td>
<td></td>
</tr>
</tbody>
</table>
ip pim register checksum

Configures the application of the checksum function on sent and received register messages in the domain.

```
ip pim register checksum {header | full}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>header</td>
<td>header</td>
</tr>
<tr>
<td>full</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

- header: Specifies that the checksum for registers is done only on the PIM header.
- full: Specifies that the checksum is done over the entire PIM register message.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900 X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The `full` option may be required for compatibility with older implementations of PIM-SM v2.
- This parameter setting must be consistent across the PIM domain.
- This command is supported only in the sparse mode.

**Examples**

```
-> ip pim register checksum header
-> ip pim register checksum full
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**show ip pim sparse**
Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

- `alaPimsmGlobalConfig`
- `alaPimsmOlRegisterMessageSupport`
**ip pim register-packing**

Enables or disables the PIM Register Message Packing.

`ip pim register-packing {enable | disable | force-enable}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the PIM register packing.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the PIM register packing.</td>
</tr>
<tr>
<td>force-enable</td>
<td>Force enables the PIM register packing</td>
</tr>
</tbody>
</table>

**Defaults**

By default, PIM register packing is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When using this command with Anycast-RP, PIM register packing should be enabled only if it is supported by all PIM anycast RP members in the RP set for the RP address.

- It is recommended to use the configuration value of "force-enable' on all the routers in the domain, when register message packing is desired and Anycast-RP is used.

- When the value “force-enable” is used, the null registers will automatically be packed without waiting for acknowledgment from an RP on whether or not the packing of register messages is supported.

- This command is supported only in the sparse mode.

**Examples**

- `-> ip pim register-packing enable`
- `-> ip pim register-packing force-enable`
- `-> ip pim register-packing disable`

**Release History**

Release 8.7R2; command was introduced.
**Related Commands**

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

- **ip pim register-mtu**
  Configures the maximum size of messages used for PIM packet register messages.

- **ip pim register-delay**
  Configures the Triggered Register Delay interval in milliseconds.

**MIB Objects**

- `alaPimsmGlobalConfig`
- `alaPimsmRegisterMsgPackingStatus`
**ip pim register-mtu**

Configures the maximum size of messages used for PIM packed register messages.

```
ip pim register-mtu num
```

**Syntax Definitions**

`num` Specify the maximum MTU size of the PIM packed register messages in bytes.

**Defaults**

By default, the value is 1500.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Before using this command, enable or force-enable PIM register packing by using the `ip pim register-packing` command.
- Use this command to configure the maximum MTU size of packed PIM register messages sent out.
- If the MTU size of the packet is larger than the interface that is used to send the packed messages, those packets may be dropped.
- It is not recommended to configure to a large value unless it is known that all the RP routers in the domain can support the MTU size in order to avoid any fragmentation and reassembly of the packets.
- This command is supported only in the sparse mode.

**Examples**

```
-> ip pim register-mtu 1000
```

**Release History**

Release 8.7R2; command was introduced.
Related Commands

show ip pim sparse
Displays the status of the various global parameters for the PIM sparse mode.

ip pim register-packing
Enables or disables the PIM Register Message Packing.

ip pim register-delay
Configures the Triggered Register Delay interval in milliseconds.

MIB Objects

alaPimsmGlobalConfig
alaPimsmPackedRegisterMsgMtu
**ip pim register-delay**

Configures the Triggered Register Delay interval in milliseconds.

`ip pim register-delay num`

---

**Syntax Definitions**

`num` Specify the Triggered Register Delay interval in milliseconds.

---

**Defaults**

By default, the value is “0”.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X48C6/T48C6/X48C4E/V48C8/C32E/T24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/X48C4E/V48C8/C32E/T24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Before using this command, enable or force-enable PIM register packing by using the `ip pim register-packing` command.

- Use this command to configure the Triggered Register Delay interval in milliseconds and to control the packing of initial bursts of triggered Null Register messages.

- This command is supported only in the sparse mode.

---

**Examples**

`-> ip pim register-delay 100`

---

**Release History**

Release 8.7R2; command was introduced.
**Related Commands**

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

- **ip pim register-packing**
  Enables or disables the PIM Register Message Packing.

- **ip pim register-mtu**
  Configures the maximum size of messages used for PIM packed register messages.

**MIB Objects**

- alaPimsmGlobalConfig
- alaPimsmPackedRegisterMsgDelay
**ip pim register-suppress-timeout**

Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.

**ip pim register-suppress-timeout seconds**

---

**Syntax Definitions**

*seconds*  
The timeout value, in seconds (0–65535).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is supported in both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

**Examples**

```
-> ip pim register-suppress-timeout 10
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ip pim sparse  Displays the status of the various global parameters for the PIM sparse mode.
show ipv6 pim sparse  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

pim
  pimRegisterSuppressionTime
**ip pim register-rate-limit**

Configures the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry.

```
ip pim register-rate-limit pps
```

---

**Syntax Definitions**

`pps`  
The per (S,G) register rate limit in packets per second (0–65535).

---

**Defaults**

By default, the register rate limit is set to zero (no rate-limiting is applied to outgoing PIM Register messages).

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/X48C4E/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Setting the register rate limit to zero (the default) disables register rate limiting.
- Rate limiting is applied on a per (S,G) flow basis.
- This command is supported in both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

---

**Examples**

```
-> ip pim register-rate-limit 100
-> ip pim register-rate-limit 0
```

---

**Release History**

Release 8.4.1.R02; command was introduced.
**Related Commands**

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

**MIB Objects**

- `alaPimsmGlobalConfigTable`
- `alaPimsmRegisterRateLimit`
**ip pim spt admin-state**

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first data packet is received.

```
ip pim spt admin-state {enable | disable}
```

**Syntax Definitions**

- **enable**
  Enables last hop DR switching to the SPT.

- **disable**
  Disables last hop DR switching to the SPT.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is supported only in the sparse mode.

- As mentioned above, if SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.

- To view whether SPT status is currently enabled (default) or disabled, use the `show ip pim sparse` command.

**Examples**

- `-> ip pim spt admin-state enable`
- `-> ip pim spt admin-state disable`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **show ip pim sparse** Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

- `alaPimsmGlobalConfig`
- `alaPimsmAdminSPTConfig`
**ip pim state-refresh-interval**

Sets the interval between successive State Refresh messages originated by a router.

**ip pim state-refresh-interval seconds**

---

**Syntax Definitions**

`seconds` The interval between successive State Refresh messages, in seconds. Values may range from 0 to 65535.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command is supported only in the dense mode.
- This value is used with both IPv4 PIM-DM and IPv6 PIM-DM.

---

**Examples**

```plaintext
-> ip pim state-refresh-interval 80
```

---

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `ip pim interface` Enables or disables the PIM protocol on a specific interface.
- `ipv6 pim interface` Enables IPv6 PIM and configures the statistics.
- `show ip pim dense` Displays the status of the various global parameters for the PIM dense mode.
- `show ipv6 pim dense` Displays the status of the various global parameters for the IPv6 PIM dense mode.

**MIB Objects**

- `pim`
  - `pimRefreshInterval`
ip pim state-refresh-limit

Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.

ip pim state-refresh-limit ticks

Syntax Definitions

ticks The limit at which the received State Refresh messages will not be forwarded, if the messages are received at less than the interval. Values may range from 0 to 65535.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ticks</td>
<td>0</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 and IPv6.

Examples

-> ip pim state-refresh-limit 2

Release History

Release 7.1.1; command was introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip pim interface</td>
<td>Enables or disables the PIM protocol on a specific interface.</td>
</tr>
<tr>
<td>ipv6 pim interface</td>
<td>Enables IPv6 PIM and configures the statistics.</td>
</tr>
<tr>
<td>show ip pim dense</td>
<td>Displays the status of the various global parameters for the PIM</td>
</tr>
<tr>
<td></td>
<td>dense mode.</td>
</tr>
<tr>
<td>show ipv6 pim dense</td>
<td>Displays the status of the various global parameters for the IPv6</td>
</tr>
<tr>
<td></td>
<td>PIM dense mode.</td>
</tr>
</tbody>
</table>

### MIB Objects

- `alaPimdmGlobalConfig`
- `alaPimdmStateRefreshLimitInterval`
ip pim state-refresh-ttl

Sets the Time to Live to be used in a router’s originated State Refresh messages if the data packet’s Time to Live is not recorded.

ip pim state-refresh-ttl num

Syntax Definitions

num The Time to Live to be used. Values may range from 0 to 255.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>16</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is supported only in the dense mode.
- This value is used with both IPv4 and IPv6 PIM-DM.

Examples

-> ip pim state-refresh-ttl 122

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **ip pim interface**
  Enables or disables the PIM protocol on a specific interface.

- **ipv6 pim interface**
  Enables IPv6 PIM and configures the statistics.

- **show ip pim dense**
  Displays the status of the various global parameters for the PIM dense mode.

- **show ipv6 pim dense**
  Displays the status of the various global parameters for the IPv6 PIM dense mode.

**MIB Objects**

- **alaPimdmGlobalConfig**
  
  - **alaPimdmStateRefreshTimeToLive**
**ip pim interface**

Enables PIM and configures PIM-related statistics such as hello-interval, triggered-hello, hello-holdtime, joinprune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the interface.

```
ip pim interface if_name
  [hello-interval seconds]
  [triggered-hello seconds]
  [joinprune-interval seconds]
  [hello-holdtime seconds]
  [joinprune-holdtime seconds]
  [prune-delay milliseconds]
  [override-interval milliseconds]
  [dr-priority priority]
  [prune-limit-interval seconds]
  [graft-retry-interval seconds]
  [df-election-robustness messages]
  [[no] stub]
  [joinprune-mtu bytes]
  [joinprune-delay milliseconds]

no ip pim interface if_name
```

**Syntax Definitions**

- `if_name`  
The interface name on which PIM is being enabled or disabled.

- `hello-interval seconds`  
The frequency at which PIM Hello messages are transmitted on a specified interface, in seconds. Values range from 0 to 18000.

- `triggered-hello seconds`  
Specifies the maximum time, in seconds, before a triggered PIM Hello message is sent on this interface. Values range from 0 to 60.

- `joinprune-interval seconds`  
The frequency at which periodic Join/Prune messages are sent on this interface, in seconds. Values range from 0 to 18000.

- `hello-holdtime seconds`  
Specifies the value set in the Holdtime field of PIM Hello messages sent on this interface, in seconds. Values range from 0 to 65535.

- `joinprune-holdtime seconds`  
The value inserted into the Holdtime field of the Join/Prune messages sent on this interface, in seconds. Values range from 0 to 65535.

- `prune-delay milliseconds`  
The value of the expected propagation delay between PIM routers on this network, inserted into the LAN prune-delay option of the Hello messages sent on this interface, in milliseconds. Values range from 0 to 32767.

- `override-interval milliseconds`  
The value inserted into the Override Interval field of the LAN prune-delay option of the Hello messages sent on this interface, in milliseconds. Values range from 0 to 65535.
**dr-priority** *priority*  
Specifies the Designated Router priority inserted into the DR priority option on a specified interface. The DR priority option value can range between 1 to 192. A higher numeric value denotes a higher priority.

**prune-limit-interval** *seconds*  
Specifies the minimum interval that must elapse between two successive prune messages sent on this interface, in seconds. Values range from 0 to 65535.

**graft-retry-interval** *seconds*  
Specifies the minimum interval that must elapse between two successive graft messages sent on this interface, in seconds. Values range from 0 to 65535.

**df-election-robustness** *messages*  
The minimum number of DF-Election messages that must be lost in order for the DF Election to fail on the specified interface. Values range from 1–65535. This value is used only by BIDIR-PIM.

**stub**  
Specifies the interface not to send any PIM packets through this interface, and to ignore received PIM packets.

**joinprune-mtu** *bytes*  
Specifies the maximum size used for PIM Join/Prune packets sent out of the interface. Values range from 0 to 9198. *Supported only on the OmniSwitch 6860 and OmniSwitch 6900.*

**joinprune-delay** *milliseconds*  
Specifies the Join/Prune delay interval in milliseconds. Values range from 0 to 32767. *Supported only on the OmniSwitch 6860 and OmniSwitch 6900.*

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello-interval <strong>seconds</strong></td>
<td>30</td>
</tr>
<tr>
<td>triggered-hello <strong>seconds</strong></td>
<td>5</td>
</tr>
<tr>
<td>joinprune-interval <strong>seconds</strong></td>
<td>60</td>
</tr>
<tr>
<td>hello-holdtime <strong>seconds</strong></td>
<td>105</td>
</tr>
<tr>
<td>joinprune-holdtime <strong>seconds</strong></td>
<td>210</td>
</tr>
<tr>
<td>prune-delay <strong>milliseconds</strong></td>
<td>500</td>
</tr>
<tr>
<td>override-interval <strong>milliseconds</strong></td>
<td>2500</td>
</tr>
<tr>
<td>dr-priority <strong>priority</strong></td>
<td>1</td>
</tr>
<tr>
<td>prune-limit-interval <strong>seconds</strong></td>
<td>60</td>
</tr>
<tr>
<td>graft-retry-interval <strong>seconds</strong></td>
<td>3</td>
</tr>
<tr>
<td>df-election-robustness <strong>messages</strong></td>
<td>3</td>
</tr>
<tr>
<td>stub</td>
<td>Disabled</td>
</tr>
<tr>
<td>joinprune-mtu <strong>bytes</strong></td>
<td>0</td>
</tr>
<tr>
<td>joinprune-delay <strong>milliseconds</strong></td>
<td>0</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to delete a PIM interface.

- PIM must be enabled globally on the switch before it runs on the interface. To globally enable or disable PIM-SM on the switch, refer to the **ip pim sparse admin-state** command on page 34-5. To enable or disable PIM-DM on the switch, refer to the **ip pim dense admin-state** command on page 34-9.

- Specifying zero for the hello-interval represents an infinite time, in which case periodic PIM Hello messages are not sent.

- Specifying zero for the joinprune-interval represents an infinite time, in which case periodic PIM Join/Prune messages are not sent.

- Specifying the value of 65535 for hello-holdtime represents an infinite time. If a PIM router gets Hello packet from a neighbor with its hello-holdtime value as infinite time, then the PIM router will not time out the sender(neighbor). It is recommended that you should use a hello-holdtime interval that is 3.5 times the value of the hello-interval, or 65535 seconds if the hello-interval is set to zero.

- Specifying the value of 65535 for joinprune-holdtime represents an infinite time. The receipt of Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite holdtime for the particular join/prune message. It is recommended that you use a joinprune-holdtime interval that is 3.5 times the value of the Join/Prune interval defined for the interface, or 65535 seconds if the joinprune-interval is set to zero.

- The interface configured as a **stub** will not send any PIM packets through that interface, and any received PIM packets are also ignored. By default, a PIM interface is not set to be a stub one.

- The **graft-retry-interval** and **prune-limit-interval** options can be used only with the PIM-DM mode.

- If the IP interface on which PIM is enabled is bound to an SPB service, then PIM can operate over an SPB L3 VPN in-line routing configuration (supported only on the OmniSwitch 9900).

- By default, **joinprune-mtu** value is ‘0’ and the configured interface MTU value will be used in determining the maximum packet size that can be used in sending the packed messages. However, if the Join/Prune MTU configuration is specified, the actual maximum size used for PIM Join/Prune messages will be the smaller of the IP MTU value of the interface and the configured interface Join/Prune MTU value.

- The **joinprune-delay** interval is used to delay the sending of triggered Join/Prune messages and may be desirable to allow the packing of triggered Join/Prune messages due to bursts of protocol messages, which may result in subsequent bursts of triggered Join/Prune packets. The default value of ‘0’ implies no deferred processing and will result in no packing of triggered Join/Prune packets.
Examples

-> ip pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-interval 100 hello-holdtime 350 joinprune-holdtime 400
-> no ip pim interface vlan-2

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **df-election-robustness** parameter added.
Release 8.6R1; **joinprune-mtu, joinprune-delay** parameters added.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip pim interface</td>
<td>Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.</td>
</tr>
</tbody>
</table>

MIB Objects

- **pimInterfaceTable**
  - pimInterfaceIfIndex
  - pimInterfaceStatus
  - pimInterfaceHelloInterval
  - pimInterfaceTrigHelloInterval
  - pimInterfaceJoinPruneInterval
  - pimInterfaceHelloHoldtime
  - pimInterfaceJoinPruneHoldtime
  - pimInterfaceDFElectionRobustness
  - pimInterfacePropagationDelay
  - pimInterfaceOverrideInterval
  - pimInterfaceDRPriority
  - pimInterfaceStubInterface
  - pimInterfacePruneLimitInterval
  - pimInterfaceGraftRetryInterval
- **alaPimInterfaceAugTable**
  - alaPimInterfaceJoinPruneMtu
  - alaPimInterfaceJoinPruneDelay
**ip pim neighbor-loss-notification-period**

Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.

```
ip pim neighbor-loss-notification-period seconds
```

### Syntax Definitions

- `seconds`: Specifies the time value that must elapse between neighbor loss notifications, in seconds (0–65535).

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The maximum value of 65535 represents an infinite time. The PIM neighbor loss notifications are never sent in case of infinite time.
- This command is used with both IPv4 and IPv6 PIM.

### Examples

```
-> ip pim neighbor-loss-notification-period 100
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

**show ip pim notifications**
Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

**MIB Objects**

| pim | pimNeighborLossNotificationPeriod |
**ip pim invalid-register-notification-period**

Specifies the minimum time that must elapse between the PIM invalid register notifications originated by the router.

**ip pim invalid-register-notification-period** seconds

---

**Syntax Definitions**

seconds Specifies the minimum time value that must elapse between invalid register notifications, in seconds (10–65535).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>65535</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The default value of 65535 represents an infinite time. The PIM invalid register notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the data and control planes to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

**Examples**

-> ip pim invalid-register-notification-period 100

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ip pim notifications*  
Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

**MIB Objects**

`pim`  
`pimInvalidRegisterNotificationPeriod`
ip pim invalid-joinprune-notification-period

Specifies the minimum time that must elapse between the PIM invalid joinprune notifications originated by the router.

`ip pim invalid-joinprune-notification-period seconds`

### Syntax Definitions

| seconds | Specifies the minimum time value that must elapse between invalid joinprune notifications, in seconds (10–65535). |

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>65535</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The default value of 65535 represents an infinite time. The PIM invalid joinprune notifications are never sent in case of infinite time.
- The non-zero minimum allowed value provides resilience against the propagation of denial-of-service attacks from the control plane to the network management plane.
- This value is used with both IPv4 and IPv6 PIM.

### Examples

```
-> ip pim invalid-joinprune-notification-period 100
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

*show ip pim notifications*  
Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

**MIB Objects**

`pim`

  `pimInvalidJoinPruneNotificationPeriod`
**ip pim rp-mapping-notification-period**

Specifies the minimum time that must elapse between the PIM RP mapping notifications originated by the router.

`ip pim rp-mapping-notification-period seconds`

---

**Syntax Definitions**

`seconds` Specifies the minimum time value that must elapse between RP mapping notifications, in seconds (0–65535).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>65535</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
No    No    No    No    Yes   Yes    Yes   Yes   Yes    Yes    Yes    Yes
```

---

**Usage Guidelines**

- The default value of 65535 represents an infinite time. The RP mapping notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

---

**Examples**

```
-> ip pim rp-mapping-notification-period 100
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

`show ip pim notifications` Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```
pim
  pimRPMappingNotificationPeriod
```
**ip pim interface-election-notification-period**

Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.

```
ip pim interface-election-notification-period seconds
```

**Syntax Definitions**

```
seconds
```

Specifies the minimum time value that must elapse between interface election notifications, in seconds (0–65535).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>65535</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The default value of 65535 represents an infinite time. The interface election notifications are never sent in case of infinite time.
- This value is used with both IPv4 and IPv6 PIM.
- This command is supported only in the sparse mode.

**Examples**

```
-> ip pim interface-election-notification-period 100
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**show ip pim notifications**  Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

```plaintext
pim
    pimInterfaceElectionNotificationPeriod
```
**ip pim nonbidir-hello-notification-period**

Specifies the minimum time that must elapse between notifications that a Bidirectional PIM (BIDIR-PIM) router transmits whenever the router receives a PIM Hello message that *does not* contain the Bidirectional Capable option.

**ip pim nonbidir-hello-notification-period** *seconds*

---

**Syntax Definitions**

*seconds*  
The minimum time value that must elapse between notifications, in seconds. The valid range is 10–65535.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>65535</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The default value of 65535 represents an infinite time. This type of notification is never sent when this value is set to infinite time.
- The default minimum time is set to a non-zero value to provide resilience against the propagation of denial-of-service (DoS) attacks from the control plane to the network management plane.
- The Bidirectional Capable option indicates that a router is capable of participating as a BIDIR-PIM neighbor.
- This value is used with both IPv4 and IPv6 PIM.
- This command is only applicable if BIDIR-PIM is globally enabled for the switch.

---

**Examples**

-> ip pim nonbidir-hello-notification-period 1000
-> ip pim nonbidir-hello-notification-period 65535

---

**Release History**

Release 7.3.4; command was introduced.
Related Commands

**ip pim df-abort**  
Configures whether or not the Designated Forwarder (DF) election process is aborted when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.

**show ip pim notifications**  
Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

MIB Objects

alaPimsmGlobalConfig  
alaPimsmNonBidirHelloPeriod
ip pim df-abort

Configures whether or not the Designated Forwarder (DF) election process is stopped when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.

```
ip pim df-abort {enable | disable}
```

---

**Syntax Definitions**

| enable     | Administratively enables the DF abort operation (DF election is stopped). |
| disable    | Administratively disables the DF abort operation (DF election is not stopped). |

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/C32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The DF election process occurs between PIM routers that support BIDIR-PIM. When the DF abort option is disabled, this election process continues between the BIDIR-PIM routers.
- This command is only applicable if BIDIR-PIM is globally enabled for the switch.

---

**Examples**

```
-> ip pim df-abort enable
-> ip pim df-abort disable
```

---

**Release History**

Release 7.3.4; command was introduced.
**Related Commands**

- **ip pim nonbidir-hello-notification-period**
  Specifies the minimum time between notifications that a BIDIR-PIM router transmits when the router receives a Hello message from a neighbor that does not contain the Bidirectional Capable option.

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

alaPimsmGlobalConfig
  - alaPimsmBidirDFAbort
**ip pim mbr all-sources**

Configures whether or not PIM notifies DVMRP about the routes to all multicast sources learned. This command applies only when the local switch is operating as a Multicast Border Router (MBR).

`ip pim mbr all-sources`

`no ip pim mbr all-sources`

---

**Syntax Definitions**

N/A

**Defaults**

By default, PIM only notifies DVMRP about the routes for subnets directly connected to PIM interfaces.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable notification of all route sources learned.
- This command applies to both PIM-SM and PIM-DM. Note that PIM-SSM does not support MBR functionality.
- DVMRP advertises the routes received from PIM within the DVMRP domain using standard DVMRP mechanisms.

**Examples**

`-> ip pim mbr all-sources`

`-> no ip pim mbr all-sources`

**Release History**

Release 7.3.2; command was introduced.
Related Commands

- `show ip pim sparse`: Displays the status of the various global parameters for the PIM sparse mode.
- `show ip pim dense`: Displays the status of the various global parameters for the PIM dense mode.
- `ip mroute mbr`: Configures the switch to operate as a Multicast Border Router to provide interoperability between PIM and DVMRP.
- `ip dvmrp interface mbr-default-information`: Configures whether or not the DVMRP interface on a Multicast Border Router advertises a default route.

MIB Objects

- `alaPimGlobalConfig`
- `alaPimMbrAllSourcesStatus`
ip pim df-periodic-interval

Sets the interval at which the Designated Forwarder (DF) for each Rendezvous Point Address (RPA) periodically announces its status in a Winner message.

`ip pim df-periodic-interval seconds`

**Syntax Definitions**

`seconds`  
The time interval between successive Winner messages, in seconds. The valid range is 0–2000.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the value for this interval is set to zero, no messages are sent.
- This value is used with both IPv4 BIRDIR-PIM and IPv6 BIRDIR-PIM.
- Setting this interval value provides an additional degree of safety to ensure that two routers do not both consider themselves to be the DF for the same link.
- The periodic Winner messages will only occur for RPAs that have active groups, thus avoiding the periodic control traffic in areas of the network without senders or receivers for a particular RPA.

**Examples**

- `-> ip pim df-periodic-interval 80`
- `-> ip pin df-periodic-interval 0`

**Release History**

Release 7.3.4; command was introduced.
**Related Commands**

- `show ip pim sparse` Displays the status of the various global parameters for the PIM sparse mode.
- `show ipv6 pim sparse` Displays the status of the various global parameters for the IPv6 PIM sparse mode.

**MIB Objects**

alaPimsmGlobalConfig
  - alaPimsmBidirPeriodicInterval
**ip pim bfd-state**

Enables or disables the registration of PIM with the BFD protocol.

```
ip pim bfd-state {enable | disable}
```

---

**Syntax Definitions**

- **enable**: Enables BFD for PIM.
- **disable**: Disables BFD for PIM.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- BFD must be globally enabled for the switch and PIM must be registered with BFD at the protocol level before PIM can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and PIM acts based upon the BFD message.
- Whenever a neighbor goes down, PIM will inform BFD to remove that neighbor from the BFD active list.

---

**Examples**

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of PIM with the BFD protocol:

```
-> ip pim bfd-state enable
-> ip pim bfd-state disable
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip bfd admin-state**
  Enables or disables the global BFD protocol status for the switch.

- **ip pim bfd-state all-interfaces**
  Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.

- **ip pim interface bfd-state**
  Enables or disables BFD monitoring on a specific PIM interface.

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

- **show ip pim dense**
  Displays the status of the various global parameters for the PIM dense mode.

MIB Objects

- **alaPimGlobal**
- **alaPimBfdStatus**
**ip pim bfd-state all-interfaces**

Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.

```
ip pim bfd-state all-interfaces {enable | disable}
```

**Syntax Definitions**

- **enable**
  - Enables BFD for all the PIM interfaces.
- **disable**
  - Disables BFD for all the PIM interfaces.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The BFD status for PIM must be enabled before PIM can interact with BFD.

**Examples**

```
-> ip pim bfd-state all-interfaces enable
-> ip pim bfd-state all-interfaces disable
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip pim bfd-state**
  - Enables or disables the registration of PIM with the BFD protocol.
- **ip pim interface bfd-state**
  - Enables or disables BFD monitoring on a specific PIM interface.
- **show ip pim interface**
  - Displays detailed PIM settings for a specific interface.

**MIB Objects**

- **alaPimGlobalConfig**
- **alaPimBfdAllInterfaceStatus**
ip pim interface bfd-state

Enables or disables BFD monitoring for a specific PIM interface.

    ip pim interface if_name bfd-state {enable | disable}

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for the specified PIM interface.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for the specified PIM interface.</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Registering PIM with BFD is required at the protocol level before PIM can interact with BFD.
- When BFD is enabled on the specified PIM interface, BFD monitors the connectivity to all neighbors known through the specified interface.

**Examples**

- `-> ip pim interface pimInt1 bfd-state enable`
- `-> ip pim interface pimInt1 bfd-state disable`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ip pim bfd-state**
Enables or disables the registration of PIM with the BFD protocol.

**ip pim bfd-state all-interfaces**
Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.

**show ip pim interface**
Displays detailed PIM settings for a specific interface.

MIB Objects

alaPimInterfaceAugTable

alaPimBfdStatus
ip pim bidir ssm-compat

Configures the status of the Source-specific Multicast (SSM) compatibility mode. When enabled, a BIDIR-PIM router will support receiving IGMPv3 SSM joins and process them as a (*,G) join.

```
ip pim bidir ssm-compat {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Administratively enables BIDIR/SSM compatibility mode.</td>
</tr>
<tr>
<td>disable</td>
<td>Administratively disables BIDIR/SSM compatibility mode.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the SSM compatibility mode is disabled, SSM joins are ignored by the BIDIR-PIM router.
- This command is only applicable if BIDIR-PIM is globally enabled for the switch.

**Examples**

- `-> ip pim bidir ssm-compat enable`
- `-> ip pim bidir ssm-compat disable`

**Release History**

Release 8.3.1.R02; command was introduced.
**Related Commands**

*show ip pim sparse*  
Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

alaPimsmGlobalConfig  
alaPimsmBidirSsmCompat
ip pim bidir fast-join

Configures whether or not a BIDIR-PIM router will automatically create (*,G) routes in the hardware as soon as BIDIR (*,G) routes are learned.

`ip pim bidir fast-join {enable | disable}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Administratively enables the BIDIR-PIM fast join functionality.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Administratively disables the BIDIR-PIM fast join functionality.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- This command is only applicable if BIDIR-PIM is globally enabled for the switch.
- When the BIDIR fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the BIDIR fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

**Examples**

- `-> ip pim bidir fast-join enable`
- `-> ip pim bidir fast-join disable`

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

- `show ip pim sparse` Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

- `alaPimsmGlobalConfig`
- `alaPimsmBidirFastJoin`
**ip pim sparse asm-fast-join**

Configures whether or not a PIM Sparse router will automatically create (*,G) routes in the hardware as soon as the (*,G) routes are learned.

```
ip pim sparse asm-fast-join {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Administratively enables the PIM Sparse ASM fast join functionality.</td>
</tr>
<tr>
<td>disable</td>
<td>Administratively disables the PIM Sparse ASM fast join functionality.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- This command is only supported in the PIM Sparse mode.
- When the PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.
- This option should be used with caution due to the complicated nature of PIM ASM, which involves forwarding on the shared tree, the sending and receiving of PIM register packets, and switching to the SPT. As a result, only enable the ASM fast join function when there are no other locally attached sources, the router is not the RP, and the SPT is disabled.

**Examples**

```
-> ip pim sparse asm-fast-join enable
-> ip pim sparse asm-fast-join disable
```

**Release History**

Release 8.3.1.R02; command was introduced.
**Related Commands**

`show ip pim sparse` Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

alaPimsmGlobalConfig
alaPimsmAsmFastJoin
ip pim sparse ssm-fast-join

Configures whether or not a PIM Sparse router will automatically create both PIM Sparse and SSM (S,G) routes in the hardware as soon as the (S,G) routes are learned.

ip pim sparse ssm-fast-join {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Administratively enables the PIM Sparse SSM fast join functionality.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Administratively disables the PIM Sparse SSM fast join functionality.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only supported in the PIM Sparse mode.
- When the PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (S,G) routes are already created before the actual multicast traffic is received.
- When the PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

Examples

- ip pim sparse ssm-fast-join enable
- ip pim sparse ssm-fast-join disable

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

show ip pim sparse Displays the status of the various global parameters for the PIM sparse mode.

MIB Objects

alaPimsmGlobalConfig
alaPimsmSsmFastJoin
**ip pim joinprune-packing**

Enable or disable PIM Join/Prune message packing.

```
ip pim joinprune-packing {enable | disable}
```

---

**Syntax Definitions**

- **enable**: Enable the PIM Join/Prune message packing.
- **disable**: Disable the PIM Join/Prune message packing.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>No</th>
<th>No</th>
<th>No</th>
<th>No</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

When this feature is disabled, Join/Prune messages are not packed.

---

**Examples**

```
-> ip pim joinprune-packing enable
-> ip pim joinprune-packing disable
```

---

**Release History**

Release 8.6R1; command introduced.

---

**Related Commands**

- **show ip pim sparse**: Displays the status of the various global parameters for the PIM sparse mode.

---

**MIB Objects**

- **alaPimGlobalConfig**
- **alaPimJoinPruneMsgPackingStatus**

---
show ip pim sparse

Displays the status of the various global parameters for the PIM sparse mode.

```
-> show ip pim sparse
Status                     = disabled,
Keepalive Period           = 210,
Max RPs                    = 32,
Probe Time                 = 5,
Register Checksum          = header,
Register Suppress Timeout  = 60,
RP Threshold               = 1,
SPT Status                 = enabled,
BIDIR Status               = disabled,
BIDIR Periodic Interval    = 60,
BIDIR DF Abort Status      = disabled,
BFD Status                 = disabled,
MoFRR Status               = disabled,
MoFRR All Routes Status    = disabled,
MBR All Sources Status     = disabled,
MBR Operational Status     = disabled,
RP Hash Algorithm          = disabled,
ASM Fast Join              = disabled,
SSM Fast Join              = disabled,
BIDIR Fast Join            = disabled,
BIDIR SSM Compatibility    = enabled,
Register Rate Limit        = 100,
```
Join/Prune Message packing = enabled,
Register Message packing = enabled,
Register MTU = 1500,
Register Triggered Delay = 200

**output definitions**

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>The current global (i.e., switch-wide) status of PIM-SM. Options include <strong>enabled</strong> and <strong>disabled</strong>.</td>
</tr>
<tr>
<td><strong>Keepalive Period</strong></td>
<td>The duration of the Keepalive timer. The default value is 210.</td>
</tr>
<tr>
<td><strong>Max RPs</strong></td>
<td>The maximum number of Rendezvous Points (RPs) allowed in the PIM-SM domain (1–100). The default value is 32.</td>
</tr>
<tr>
<td><strong>Probe Time</strong></td>
<td>The amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP. Values may range from 1 to 300. The default value is 5.</td>
</tr>
<tr>
<td><strong>Register Checksum</strong></td>
<td>The current application of the checksum function on register messages in the domain. Options include <strong>header</strong> and <strong>full</strong>. The default setting is <strong>header</strong>.</td>
</tr>
<tr>
<td><strong>Register Suppress Timeout</strong></td>
<td>The amount of time, in seconds, the Designated Router (DR) will stop sending registers to the Rendezvous Point (RP) once a Register-Stop is received (1–300). The default value is 60.</td>
</tr>
<tr>
<td><strong>RP Threshold</strong></td>
<td>Displays the current RP data rate threshold. This value indicates the rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing an (S, G) Join message toward the source. Values may range from 0 to 2147483647. The default value is 1. A value of 0 indicates that the feature is currently disabled.</td>
</tr>
<tr>
<td><strong>SPT Status</strong></td>
<td>The current status of last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). Options include <strong>enabled</strong> (the default) and <strong>disabled</strong>.</td>
</tr>
<tr>
<td><strong>BIDIR Status</strong></td>
<td>The current global status of Bidirectional PIM (BIDIR-PIM) for the switch. Options include <strong>enabled</strong> and <strong>disabled</strong> (the default).</td>
</tr>
<tr>
<td><strong>BIDIR Periodic Interval</strong></td>
<td>The amount of time, in seconds, between Winner messages the Designated Forwarder (DF) sends out to announce its status. The valid range is 0–2000. The default is 60 seconds.</td>
</tr>
<tr>
<td><strong>BIDIR DF Abort Status</strong></td>
<td>Indicates whether or not the DF election process is stopped when a BIDIR-PIM router receives a Hello message that does not contain the Bidirectional Capable option. When <strong>enabled</strong> DF election is stopped; when <strong>disabled</strong> (the default) DF election continues.</td>
</tr>
<tr>
<td><strong>BFD Status</strong></td>
<td>Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is <strong>enabled</strong> or <strong>disabled</strong> (the default) for the PIM router.</td>
</tr>
<tr>
<td><strong>MoFRR Status</strong></td>
<td>Not supported in the current release.</td>
</tr>
<tr>
<td><strong>MoFRR All Routes Status</strong></td>
<td>Not supported in the current release.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBR All Sources Status</td>
<td>Indicates whether or not PIM notifies DVMRP about the routes to all multicast sources learned. Options include <strong>enabled</strong> (routes to all sources) or <strong>disabled</strong> (only routes on PIM interfaces). This status only applies when the switch is operating in the Multicast Border Router (MBR) mode.</td>
</tr>
<tr>
<td>MBR Operational Status</td>
<td>Indicates whether or not PIM interaction with DVMRP is <strong>enabled</strong> or <strong>disabled</strong> on a MBR switch. MBR functionality is not operationally active until both PIM and DVMRP have at least one enabled and active interface.</td>
</tr>
<tr>
<td>RP Hash Algorithm</td>
<td>The status of the RP hashing algorithm. When <strong>enabled</strong>, a newer version of the algorithm is in use; when <strong>disabled</strong> (the default), a legacy version of the algorithm is in use.</td>
</tr>
<tr>
<td>ASM Fast Join</td>
<td>PIM Sparse fast join is not supported.</td>
</tr>
<tr>
<td>SSM Fast Join</td>
<td>PIM Sparse fast join is not supported.</td>
</tr>
<tr>
<td>BIDIR Fast Join</td>
<td>BIDIR-PIM fast join is not supported.</td>
</tr>
<tr>
<td>BIDIR SSM Compatibility</td>
<td>The status of the SSM compatibility mode. When <strong>enabled</strong>, a BIDIR-PIM router will accept and process SSM joins as (*,G) joins; when <strong>disabled</strong> (the default), SSM joins are ignored.</td>
</tr>
<tr>
<td>Register Rate Limit</td>
<td>The per (S,G) register rate limit in packets per second.</td>
</tr>
<tr>
<td>Join/Prune Message Packing</td>
<td>The current status of PIM Join/Prune message packing. Options include <strong>enabled</strong> and <strong>disabled</strong>.</td>
</tr>
<tr>
<td>Register Message Packing</td>
<td>The current status of PIM Register message packing. Options include <strong>enabled</strong>, <strong>force-enabled</strong> and <strong>disabled</strong>.</td>
</tr>
<tr>
<td>Register MTU</td>
<td>The size of the message in bytes used for PIM packed register messages.</td>
</tr>
<tr>
<td>Register Trigger Delay</td>
<td>The Triggered Register Delay interval in milliseconds.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; **MBR All Sources Status** and **MBR Operational Status** fields added.
Release 7.3.4; BIDIR fields added, **RP Hash Algorithm** field added.
Release 8.4.1.R02; **Register Rate Limit** field added.
Release 8.6R1; **Join/Prune Message Packing** field added.
Release 8.7R2; **Register Message Packing**, **Register MTU**, **Register Trigger Delay** fields added.
### Related Commands

- **ip pim sparse admin-state**
  Globally enables or disables PIM-SM protocol on the switch.

- **ip pim interface**
  Enables or disables the PIM protocol on a specific interface.

- **ip pim keepalive-period**
  Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.

- **ip pim max-rps**
  Configures the maximum number of C-RP routers allowed in the PIM-SM domain.

- **ip pim probe-time**
  Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.

- **ip pim register checksum**
  Configures the application of the checksum function on sent and received register messages in the domain.

- **ip pim register-suppress-timeout**
  Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.

- **ip pim register-rate-limit**
  Specifies the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry.

- **ip pim rp-threshold**
  Specifies the data rate, in bits per second (bps), at which the Rendezvous Point (RP) will attempt to switch to native forwarding by issuing a source-specific (S,G) Join message toward the source.

- **ip pim spt admin-state**
  Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first data packet is received.

- **ip pim bidir admin-state**
  Globally enables or disables BIDIR-PIM protocol on the switch.

- **ip pim df-periodic-interval**
  Configures the time interval at which the DF for each RP address periodically announces its status in a Winner message.

- **ip pim df-abort**
  Configures whether or not the DF election process is stopped when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.

- **ip pim bfd-state**
  Enables or disables the registration of PIM with the BFD protocol.

- **ip pim mbr all-sources**
  Configures PIM to notify DVMRP of all learned routes to sources. This command only applies when the switch is operating in the Multicast Border Router mode.

- **ip pim rp-hash admin-state**
  Globally enables or disables the RP hashing algorithm version.

- **ip pim bidir ssm-compat**
  Configures the SSM compatibility mode for a BIDIR-PIM router.

- **ip pim joinprune-packing**
  Enable or disable PIM Join/Prune message packing.

- **ip pim register-packing**
  Enables or disables the PIM Register Message Packing.

- **ip pim register-mtu**
  Configures the maximum size of messages used for PIM packed register messages.

- **ip pim register-delay**
  Configures the Triggered Register Delay interval in milliseconds.
MIB Objects

ALCATEL-IND1-PIM-MIB
alaPimsmGlobalConfig
alaPimsmAdminStatus
alaPimsmMaxRPS
alaPimsmProbeTime
alaPimsmOldRegisterMessageSupport
alaPimsmRPThreshold
alaPimsmAdminSPTConfig
alaPimsmBidirStatus
alaPimsmBidirPeriodicInterval
alaPimsmBidirDFAbort
alaPimMbrAllSourcesStatus
alaPimMbrOperStatus
alaPimsmRPHashStatus
alaPimsmAsmFastJoin
alaPimsmSsmFastJoin
alaPimsmBidirFastJoin
alaPimsmBidirSsmCompat
alaPimsmRegisterRateLimit
alaPimsmRegisterMsgPackingStatus
alaPimsmRegisterMsgPackingStatus
alaPimsmPackedRegisterMsgDelay
alaPimGlobalConfig
alaPimBfdStatus
alaPimJoinPruneMsgPackingStatus
alaPimGlobalConfig
alaPimsmRegisterMsgPackingStatus
alaPimsmV6RegisterMsgPackingStatus
PIM-STD-MIB
pim
pimKeepalivePeriod
pimRegisterSuppressionTime
show ip pim dense

Displays the status of the various global parameters for the PIM dense mode.

show ip pim dense

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

```
-> show ip pim dense
Status             = enabled,
Source Lifetime    = 210,
State Refresh Interval = 60,
State Refresh Limit Interval = 0,
State Refresh TTL  = 16,
BFD Status         = disabled,
MoFRR Status       = disabled,
MBR All Sources Status = disabled,
MBR Operational Status = enabled
```

output definitions

<table>
<thead>
<tr>
<th>Status</th>
<th>The current global (i.e., switch-wide) status of PIM-DM. Options include enabled and disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Lifetime</td>
<td>The duration of the Keepalive or Source Lifetime timer. The default value is 210.</td>
</tr>
<tr>
<td>State Refresh Interval</td>
<td>The time-interval, in seconds, between successive State Refresh messages originated by the router. The default value is 60.</td>
</tr>
<tr>
<td>State Refresh Limit Interval</td>
<td>Displays the limit at which a router will not forward the State Refresh messages, if they are received at less than the interval.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State Refresh TTL</td>
<td>Displays the TTL to be used in the router’s originated State Refresh messages. The default value is 16.</td>
</tr>
<tr>
<td>BFD Status</td>
<td>Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is enabled or disabled (the default) for the PIM router.</td>
</tr>
<tr>
<td>MoFRR Status</td>
<td>Not supported in the current release.</td>
</tr>
<tr>
<td>MBR All Sources Status</td>
<td>Indicates whether or not PIM notifies DVMRP about the routes to all multicast sources learned. Options include enabled (routes to all sources) or disabled (only routes on PIM interfaces). This status only applies when the switch is operating in the Multicast Border Router (MBR) mode.</td>
</tr>
<tr>
<td>MBR Operational Status</td>
<td>Indicates whether or not PIM interaction with DVMRP is enabled or disabled on a MBR switch. MBR functionality is not operationally active until both PIM and DVMRP have at least one enabled and active interface.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.2; MBR All Sources Status and MBR Operational Status fields added.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip pim dense admin-state</td>
<td>Globally enables or disables PIM-DM protocol on the switch.</td>
</tr>
<tr>
<td>ip pim interface</td>
<td>Enables or disables the PIM protocol on a specific interface.</td>
</tr>
<tr>
<td>ip pim state-refresh-interval</td>
<td>Sets the interval between successive State Refresh messages originated by a router.</td>
</tr>
<tr>
<td>ip pim state-refresh-limit</td>
<td>Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.</td>
</tr>
<tr>
<td>ip pim state-refresh-ttl</td>
<td>Sets the Time to Live to be used in a router’s originated State Refresh messages if the data packet’s Time to Live is not recorded.</td>
</tr>
<tr>
<td>ip pim keepalive-period</td>
<td>Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.</td>
</tr>
<tr>
<td>ip pim bfd-state</td>
<td>Enables or disables the registration of PIM with the BFD protocol.</td>
</tr>
<tr>
<td>ip pim mbr all-sources</td>
<td>Configures PIM to notify DVMRP of all learned routes to sources. This command only applies when the switch is operating in the Multicast Border Router mode.</td>
</tr>
</tbody>
</table>
**MIB Objects**

ALCATEL-IND1-PIM-MIB.mib
alaPimdmGlobalConfig
  alaPimdmAdminStatus
  alaPimRefreshInterval
  alaPimdmStateRefreshLimitInterval
  alaPimdmStateRefreshTimeToLive
  alaPimMbrAllSourcesStatus
  alaPimMbrOperStatus

alaPimGlobalConfig
  alaPimBfdStatus

PIM-STD-MIB.mib

pim
  pimKeepalivePeriod
show ip pim ssm group

Displays the static configuration of multicast group mappings for the PIM-Source Specific Multicast (SSM) mode.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only in the sparse mode.

Examples

-> show ip pim ssm group

<table>
<thead>
<tr>
<th>Group Address/Prefix</th>
<th>RP Address</th>
<th>Mode</th>
<th>Override</th>
<th>Precedence</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.0.0/24</td>
<td>0.0.0.0</td>
<td>ssm</td>
<td>false</td>
<td>none</td>
<td>enabled</td>
</tr>
</tbody>
</table>

output definitions

- **Group Address/Prefix**: The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
- **RP Address**: A 32-bit IP address that is the Rendezvous Point (RP) for groups within the group prefix.
- **Mode**: The PIM mode to be used for groups in this prefix. The possible values include *asm*, *ssm*, or *dm*.
- **Override**: Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
**Output Definitions**

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Specifies the precedence value to be used for this static RP configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays whether this entry is currently enabled or disabled. Options include <code>enabled</code> and <code>disabled</code>.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **`ip pim ssm group`**
  
  Statically maps the specified IP multicast group(s) to the PIM Source Specific Multicast mode (SSM).

- **`show ip pim group-map`**
  
  Displays the PIM group mapping table.

**MIB Objects**

- `pimStaticRPTable`
  
  - `pimStaticRPGrpAddress`
  - `pimStaticRPGrpPrefixLength`
  - `pimStaticRPRAAddress`
  - `pimStaticRPImMode`
  - `pimStaticRP OverrideDynamic`
  - `pimStaticRPPrecedence`
  - `pimStaticRPRowStatus`
**show ip pim dense group**

Displays the static configuration of multicast group mappings for PIM-Dense Mode (DM).

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/X48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- This command is supported only on PIM dense mode.

**Examples**

```
-> show ip pim dense group
Group Address/Prefix RP Address          Mode  Override Precedence Status
---------------------------------------------------------------
225.0.0.0/24       0.0.0.0   dm    false    none       enabled
```

**output definitions**

- **Group Address/Prefix**: The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).
- **Mode**: The PIM mode to be used for groups in this prefix. The possible values include asm, ssm, or dm.
- **RP Address**: A 32-bit IP address that is the Rendezvous Point (RP) for groups within the group prefix.
- **Override**: Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
**output definitions**

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Specifies the precedence value to be used for this static RP configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays whether this entry is currently enabled or disabled. Options include <strong>enabled</strong> and <strong>disabled</strong>.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ip pim dense group**: Creates and manages the static configuration of dense mode (DM) group mappings.
- **show ip pim group-map**: Displays the PIM group mapping table.

**MIB Objects**

- `alaPimdmDenseGroupTable`
  - `alaPimdmDenseGroupGrpAddress`
  - `alaPimdmDenseGroupGrpPrefixLength`
  - `alaPimdmDenseGroupOverrideDynamic`
  - `alaPimdmDenseGroupPrecedence`
  - `alaPimdmDenseGroupRowStatus`
show ip pim neighbor

Displays a list of active PIM neighbors.

**show ip pim neighbor [ip_address]**

**Syntax Definitions**

*ip_address*  
The 32-bit IP address for the PIM neighbor.

**Defaults**

If a neighbor’s IP address is not specified, the entire PIM neighbor table is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view more detailed information about a particular neighbor, specify the neighbor's IP address in the command line. Additional information will be displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

**Examples**

```
-> show ip pim neighbor
Neighbor Address    Interface Name    Uptime       Expires      DR Priority
-----------------+--------------------+-----------+-----------+-------------
212.61.20.250      vlan-2            01h:07m:07s 00h:01m:38s 100
212.61.60.200      vlan-6            01h:07m:07s 00h:01m:38s 100
214.28.4.254       vlan-26           01h:07m:07s 00h:01m:38s 100
```

If a specific neighbor IP address is specified in the command line, *detailed information for the corresponding neighbor only* displays:

```
-> show ip pim neighbor 212.61.30.7
Neighbor IP Address  = 212.61.30.7,
Interface Name       = vlan-30,
Uptime               = 00h:04m:14s,
Expires              = 00h:01m:31s,
Lan Prune Delay Present = true,
Propagation Delay    = 500,
Override Interval    = 2500,
TBit field           = false,
Gen ID Present       = true,
```
Gen ID Value = 0x79ca868e,
BiDir Capable = false,
DR Priority Present = true,
DR Priority = 1,
State Refresh Capable = true

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor (IP) Address</td>
<td>The 32-bit IP address of the active PIM neighbor.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The name of the interface used to reach this PIM neighbor.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Expiry time</td>
<td>The minimum amount of time remaining before the PIM neighbor will be aged out, displayed in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Lan Prune Delay Present</td>
<td>Evaluates to TRUE if this neighbor is using the Lan Prune Delay option.</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>The expected propagation delay between PIM routers on this network.</td>
</tr>
<tr>
<td>DR Priority Present</td>
<td>Evaluates to TRUE if the neighbor is using the DR Priority option.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>The value of the Designated Router Priority from the last PIM Hello message received from this neighbor. This object is always zero if the DR Priority Present value is FALSE.</td>
</tr>
<tr>
<td>TBit field</td>
<td>The value of the Tbit field of the LAN prune delay option received from this neighbor. The Tbit specifies the ability of the neighbor to disable Join suppression.</td>
</tr>
<tr>
<td>Generation ID Present</td>
<td>Evaluates to TRUE if this neighbor is using the Generation ID option.</td>
</tr>
<tr>
<td>Generation ID Value</td>
<td>The value of the Generation ID from the last PIM Hello message received from the neighbor.</td>
</tr>
<tr>
<td>BiDir Capable</td>
<td>Evaluates to TRUE if this neighbor is using the Bidirectional-PIM Capable option.</td>
</tr>
<tr>
<td>State Refresh Capable</td>
<td>Displays whether the neighbor is capable of receiving State Refresh messages. Options include true or false.</td>
</tr>
<tr>
<td>Override Interval</td>
<td>The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
**Related Commands**

*show ip pim interface*  
Displays the PIM interface configuration.

**MIB Objects**

`pimNeighborTable`

- `pimNeighborIfIndex`
- `pimNeighborAddressType`
- `pimNeighborAddress`
- `pimNeighborGenerationIDPresent`
- `pimNeighborGenerationIDValue`
- `pimNeighborUpTime`
- `pimNeighborExpiryTime`
- `pimNeighborDRPriorityPresent`
- `pimNeighborDRPriority`
- `pimNeighborLanPruneDelayPresent`
- `pimNeighborTBit`
- `pimNeighborPropagationDelay`
- `pimNeighborOverrideInterval`
- `pimNeighborBidirCapable`
- `pimNeighborSRCapable`
show ip pim candidate-rp

Displays the IP multicast groups for which the local router advertises itself as a Candidate-RP.

show ip pim candidate-rp

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> show ip pim candidate-rp
RP Address  Group Address  Priority  Interval  Mode  Status
---------------------------------------------------------------
40.1.50.25  225.0.0.0/8  192       60       bidir enabled

**output definitions**

**RP Address**
A 32-bit IP address that is advertised as the Candidate-Rendezvous Point (RP).

**Group Address**
The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash character (/). This is the group for which the local router advertises itself as a C-RP.

**Priority**
The C-RP router’s priority. The lower the value, the higher the priority.

**Interval**
The time interval at which the C-RP advertisements are sent to the BSR.
**output definitions**

<table>
<thead>
<tr>
<th>Mode</th>
<th>Whether or not the Group Address is for a PIM-SM group or a Bidirectional PIM (BIDIR-PIM) group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.  
Release 7.3.4; **Mode** field added.

**Related Commands**

**ip pim candidate-rp**  
Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IP multicast group(s).

**MIB Objects**

pimBsrCandidateRPTable  
pimBsrCandidateRPAAddressType  
pimBsrCandidateRPAAddress  
pimBsrCandidateRPGroupAddress  
pimBsrCandidateRPGroupPrefixLength  
pimBsrCandidateRPBidir  
pimBsrCandidateRPAdvTimer  
pimBsrCandidateRPPriority  
pimBsrCandidateRPAdvInterval  
pimBsrCandidateRPHoldtime  
pimBsrCandidateRPPriority  
pimBsrCandidateRPStorageType
show ip pim group-map

Displays the PIM group mapping table.

show ip pim group-map [bsr | static-rp | ssm | dense]

Syntax Definitions

N/A

Defaults

If the keywords bsr, static-rp, ssm, or dense are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the ip pim static-rp command. As long as the RP addresses defined in the static RP set are reachable, they will be added to the group mapping table.

- If the IP multicast groups are mapped to the mode SSM or DM, then the entries created by local SSM address range configuration using the ip pim ssm group command and local Dense Mode address range configuration using the ip pim dense group command are displayed.

- If the bootstrap mechanism is being used, this information is obtained from received Candidate-RP advertisements (when the local router is the BSR; when the local router is not the BSR, this information is obtained from received bootstrap messages).

Examples

```bash
-> show ip pim group-map
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+---------------------------+-------------+-----+-----------
BSR       225.0.0.0/24                172.21.63.11  asm   192
BSR       225.0.0.0/8                 40.1.50.25    bidir 192
Static RP 226.0.0.0/8                 10.11.203.8   bidir none
Static RP 232.0.0.0/8                               ssm

-> show ip pim group-map bsr
Origin    Group Address/Pref Length   RP Address    Mode  Precedence
---------+---------------------------+-------------+-----+-----------
BSR       225.0.0.0/24                172.21.63.11  asm   192
```
BSR       225.0.0.0/24                214.0.0.7     asm   192
BSR       225.0.0.0/8                 40.1.50.25    bidir 192

-> show ip pim group-map static-rp

<table>
<thead>
<tr>
<th>Origin</th>
<th>Group Address/Pref Length</th>
<th>RP Address</th>
<th>Mode</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static RP 226.0.0.0/8</td>
<td>10.11.203.8</td>
<td>bidir  none</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static RP 232.0.0.0/8</td>
<td>ssm</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Output definitions

**Origin**
The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.

**Group Address/Prefix Length**
The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/).

**RP Address**
The IP address of the Rendezvous Point to be used for groups within the group prefix. There is no RP address if the PIM mode is either SSM or DM.

**Mode**
The PIM mode to be used for groups in this prefix.

**Mapping Precedence**
The precedence value of a particular row, which determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; bidir mode support added.

Related Commands

**ip pim ssm group**
Creates and manages the static configuration of a Source Specific Multicast mode group mappings.

**ip pim dense group**
Creates and manages the static configuration of dense mode (DM) group mappings.

**ip pim static-rp**
Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

MIB Objects

pimGroupMappingTable
  pimGroupMappingOrigin
  pimGroupMappingAddressType
  pimGroupMappingGrpAddress
  pimGroupMappingGrpPrefixLength
  pimGroupMappingRPAddressType
  pimGroupMappingRPAddress
  pimGroupMappingPimMode
pimGroupMappingPrecedence


show ip pim interface

Displays detailed PIM settings for a specific interface. In general, it displays PIM settings for all the interfaces if no argument is specified.

show ip pim interface [if_name]

Syntax Definitions

if_name

The interface name.

Defaults

By default, displays a summary list of IP PIM interfaces.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

Examples

-> show ip pim interface

Total 1 Interfaces

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>IP Address</th>
<th>Designated Router</th>
<th>Hello Interval</th>
<th>J/P</th>
<th>Oper</th>
<th>BFD</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-203</td>
<td>11.12.203.8</td>
<td>11.12.203.8</td>
<td>30</td>
<td>60</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

disabled        |

-> show ip pim interface vlan-203

Interface Name  = vlan-203,
IP Address      = 11.12.203.8,
Designated Router = 11.12.203.8,
Hello Interval  = 30,
Triggered Hello Interval = 5,
Hello HoldTime  = 105,
Join/Prune Interval = 60,
Join/Prune HoldTime = 210,
Propagation (Prune) Delay = 500,
Override Interval = 2500,
show ip pim interface

Generation ID               = 0x53291e4c,
DR Priority                 = 1,
DR Priority Enabled         = true,
Lan Delay Enabled           = true,
Effective Propagation Delay = 500,
Effective Override Interval = 2500,
Suppression Enabled         = true,
Stub Interface              = false,
Prune Limit Interval        = 60,
Graft Retry Interval        = 3,
State Refresh Enabled       = true,
BiDir Capable               = false,
DF Election Robustness      = 3,
Operational Status          = disabled,
BFD Status                  = disabled,
Join/Prune MTU              = 1000,
Join/Prune Triggered Delay  = 100

output definitions

Interface Name            The name of the interface on which PIM is enabled.
IP address                Specifies the IP address of the specified interface.
Designated Router         The 32-bit IP address for the Designated Router (DR). The DR acts on behalf of any directly-connected hosts with respect to the PIM-SM protocol. Only one router in the LAN will act as the DR.
Hello Interval            The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.
Triggered Hello Interval   The current Triggered Hello Interval. This value indicates the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface. Values may range from 1 to 60. The default value is 5.
Hello Holdtime            The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.
Join/Prune Interval        The Join/Prune interval for the associated interface. The Join/Prune interval is the interval at which periodic PIM-SM Join/Prune messages are sent. Values may range from 1 to 18000.
Join/Prune Holdtime        The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.
Propagation (Prune) Delay  The expected propagation delay between PIM routers on this network.
Override Interval          The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Generation ID</strong></td>
<td>The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.</td>
</tr>
<tr>
<td><strong>DR Priority</strong></td>
<td>Displays the Designated Router priority for each interface. This value is used in determining the Designated Router on an interface. Values may range from 1 to 192. A higher numeric value denotes a higher priority. Note that priority-based election is used only if all routers on the interface are using the DR priority option. The default value is 1.</td>
</tr>
<tr>
<td><strong>DR Priority Enabled</strong></td>
<td>Evaluates to TRUE if all routers on this interface are using the DR Priority option.</td>
</tr>
<tr>
<td><strong>Lan Delay Enabled</strong></td>
<td>Options include true and false. The value will be true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting will be false.</td>
</tr>
<tr>
<td><strong>Effective Propagation Delay</strong></td>
<td>The Effective Propagation Delay on this interface.</td>
</tr>
<tr>
<td><strong>Effective Override Interval</strong></td>
<td>The Effective Override Interval on this interface.</td>
</tr>
<tr>
<td><strong>Suppression Enabled</strong></td>
<td>Specifies whether the Join suppression is enabled on this interface.</td>
</tr>
<tr>
<td><strong>Stub Interface</strong></td>
<td>Specifies whether this interface is a 'stub interface'. If this is TRUE, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.</td>
</tr>
<tr>
<td><strong>Prune Limit Interval</strong></td>
<td>The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM.</td>
</tr>
<tr>
<td><strong>Graft Retry Interval</strong></td>
<td>Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is used only with PIM-DM. Values may range from 1 to 65535. The default value is 3.</td>
</tr>
<tr>
<td><strong>State Refresh Enabled</strong></td>
<td>Evaluates to TRUE if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.</td>
</tr>
<tr>
<td><strong>BiDir Capable</strong></td>
<td>Evaluates to TRUE if all routers on this interface are using the Bidirectional Capable option. This is used only by BIDIR-PIM.</td>
</tr>
<tr>
<td><strong>DF Election Robustness</strong></td>
<td>The minimum number of PIM Designated Forwarder (DF) Election messages that must be lost to determine that the DF Election process has failed for this interface. This is used only by BIDIR-PIM.</td>
</tr>
<tr>
<td><strong>Operational Status</strong></td>
<td>The current operational status of the corresponding interface. Options include enabled and disabled. This value indicates whether the IP interface is operationally up. For example, if PIM is enabled on the interface, but the IP interface is currently down, this field will display as disabled. The default setting is disabled. To globally enable or disable PIM on the switch, use the ip pim sparse admin-state and ip pim dense admin-state commands.</td>
</tr>
<tr>
<td><strong>BFD Status</strong></td>
<td>Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is enabled or disabled (the default) for the PIM interface. Configured through the ip pim interface bfd-state command.</td>
</tr>
<tr>
<td><strong>Join/Prune MTU</strong></td>
<td>The configured PIM Join/Prune packet MTU for this interface.</td>
</tr>
<tr>
<td><strong>Join/Prune Triggered Delay</strong></td>
<td>The triggered Join/Prune delay.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; **BiDir Capable** and **DF Election Robustness** fields added.
Release 8.6R1; **Join/Prune MTU** and **Join/Prune Triggered** Delay fields added.

**Related Commands**

- `ip pim interface` Enables or disables the PIM protocol on a specific interface.

**MIB Objects**

- `pimInterfaceTable`
  - `pimInterfaceIFIndex`
  - `pimInterfaceIPvVersion`
  - `pimInterfaceAddressType`
  - `pimInterfaceAddress`
  - `pimInterfaceGenerationIDValue`
  - `pimInterfaceDR`
  - `pimInterfaceDRPriority`
  - `pimInterfaceDRPriorityEnabled`
  - `pimInterfaceHelloInterval`
  - `pimInterfaceTrigHelloInterval`
  - `pimInterfaceHelloHoldtime`
  - `pimInterfaceJoinPruneInterval`
  - `pimInterfaceJoinPruneHoldtime`
  - `pimInterfaceDFElectionRobustness`
  - `pimInterfaceLanDelayEnabled`
  - `pimInterfacePropagationDelay`
  - `pimInterfaceOverrideInterval`
  - `pimInterfaceEffectPropagDelay`
  - `pimInterfaceEffectOverrideIvl`
  - `pimInterfaceSuppressionEnabled`
  - `pimInterfaceBidirCapable`
  - `pimInterfaceDomainBorder`
  - `pimInterfaceStubInterface`
  - `pimInterfacePruneLimitInterval`
  - `pimInterfaceGraftRetryInterval`
  - `pimInterfaceSRPriorityEnabled`
  - `pimInterfaceStatus`

- `alaPimInterfaceAugTable`
  - `alaPimInterfaceBfdStatus`
  - `alaPimInterfaceJoinPruneMtu`
  - `alaPimInterfaceJoinPruneDelay`
show ip pim static-rp

Displays the PIM Static RP table for the ASM mode, which includes group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (i.e., enabled or disabled).

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

-> show ip pim static-rp

<table>
<thead>
<tr>
<th>Group Address/Pref Length</th>
<th>RP Address</th>
<th>Mode</th>
<th>Override Precedence</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.0.0/24</td>
<td>172.21.63.11</td>
<td>asm</td>
<td>false</td>
<td>enabled</td>
</tr>
<tr>
<td>226.0.0.0/8</td>
<td>10.11.203.8</td>
<td>bidir</td>
<td>false</td>
<td>enabled</td>
</tr>
</tbody>
</table>

output definitions

Group Address/Pref Length: The 32-bit IP address for a multicast group, along with the mask length, shown in bits. The group IP address and mask are separated by a slash (/). To change the current multicast group address and mask, refer to the `ip pim static-rp` command on page 34-19.

RP Address: A 32-bit IP address of the Rendezvous Point (RP). To change the current RP address, refer to the `ip pim static-rp` command on page 34-19.

Mode: The PIM mode to be used for groups in this prefix. The possible values include `asm`, `ssm`, or `bidir`. 
### Output Definitions

<table>
<thead>
<tr>
<th>Override</th>
<th>Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precedence</td>
<td>Specifies the precedence value to be used for this static RP configuration.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays whether static RP configuration is currently enabled or disabled. Options include enabled and disabled. To change the current status, refer to the <code>ip pim static-rp</code> command.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command was introduced.
Release 7.3.4: `bidir` mode support added.

### Related Commands

**ip pim static-rp**

Adds, modifies, or deletes a static RP for a group (“modifies” applies only to the RP address, since the table is indexed from group address and mask parameters).

### MIB Objects

- `pimStaticRPTable`
  - `pimStaticRPAddressType`
  - `pimStaticRPGrpAddress`
  - `pimStaticRPGrpPrefixLength`
  - `pimStaticRPRPAddress`
  - `pimStaticRPImMode`
  - `pimStaticRPOverrideDynamic`
  - `pimStaticRPPrecedence`
  - `pimStaticRPRowStatus`
  - `pimStaticRPStorageType`
**show ip pim anycast-rp**

Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration.

**show ip pim anycast-rp**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

**Examples**

```
-> show ip pim anycast-rp
Anycast RP Address     Router Address     Local     Status
-------------------------------+-------------------+--------+---------
10.10.10.1                10.1.1.2          true    enabled
10.10.10.1                10.1.2.2          false   enabled
```

**output definitions**

- **Anycast RP Address**: The anycast RP address.
- **Router Address**: The router IP address that is a member of the anycast RP set.
- **Local**: Displays whether this entry corresponds to the local router. The value will display true if this entry corresponds to the local router and false if it does not correspond to the local router.
- **Status**: Displays whether the anycast RP configuration is currently enabled or disabled. To change the current status, refer to the `ip pim anycast-rp` command.
Release History

Release 8.6R2; command introduced.

Related Commands

ip pim anycast-rp

Configures the anycast RP set, which is the set of all routers that would act as the RP.

MIB Objects

pimAnycastRPSetsTable
  pimAnycastRPSetsAddressType
  pimAnycastRPSetsAnycastAddress
  pimAnycastRPSetsRouterAddress
  pimAnycastRPSetsLocalRouter
  pimAnycastRPSetsRowStatus
**show ip pim cbsr**

Displays the Candidate-BSR information that is used in the Bootstrap messages.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```bash
-> show ip pim cbsr
CBSR Address       = 214.0.0.7,
Status              = enabled,
CBSR Priority       = 0,
Hash Mask Length    = 30,
Elected BSR         = False,
Timer               = 00h:00m:00s
```

**output definitions**

<table>
<thead>
<tr>
<th>CBSR Address</th>
<th>The 32-bit address that the local router uses to advertise itself as a Candidate-BSR.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The current status of this entry. The status is shown as enabled only if the PIM-SM is globally enabled and the PIM interface is enabled.</td>
</tr>
<tr>
<td>CBSR Priority</td>
<td>The value for the local router as a Candidate-BSR. The higher the value, the higher the priority.</td>
</tr>
<tr>
<td>Hash Mask Length</td>
<td>The 32-bit mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group.</td>
</tr>
</tbody>
</table>
### Output Definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Elected BSR</strong></td>
<td>Specifies whether the local router is the elected BSR.</td>
</tr>
<tr>
<td><strong>Timer</strong></td>
<td>The time value that is remaining before the local router originates the next bootstrap message. This value is zero if this router is not the elected BSR.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command was introduced.

### Related Commands

**ip pim cbsr**  
Configures the Candidate-BSR information that is used in the Bootstrap messages.

### MIB Objects

- **pimBSrCandidateBSRTable**
  - **pimBsrCandidateBSRZoneIndex**
  - **pimBsrCandidateBSRAddressType**
  - **pimBsrCandidateBSRAddress**
  - **pimBsrCandidateBSRPriority**
  - **pimBsrCandidateBSRHashMaskLength**
  - **pimBsrCandidateBSRElectedBSR**
  - **pimBsrCandidateBSRBootstrapTimer**
  - **pimBsrCandidateBSRStatus**
**show ip pim bsr**

Displays information about the elected BSR.

```
show ip pim bsr
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ip pim bsr
BSR Address        = 214.0.0.7
BSR Priority       = 192,
Hash Mask Length   = 30,
Expiry Time        = 00h:01m:35s
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSR Address</td>
<td>The 32-bit address of the elected BSR.</td>
</tr>
<tr>
<td>BSR Priority</td>
<td>The priority value of the elected BSR. The higher the value, the higher the priority.</td>
</tr>
<tr>
<td>Hash Mask Length</td>
<td>The 32-bit mask length that is advertised in the bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group).</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>The minimum time remaining before the elected BSR will be declared down.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ip pim cbsr**

Configures the Candidate-BSR information that is used in the Bootstrap messages.

MIB Objects

```plaintext
pimBsrElectedBSRTable
   pimBsrElectedBSRZoneIndex
   pimBsrElectedBSRAddressType
   pimBsrElectedBSRAddress
   pimBsrElectedBSRPriority
   pimBsrElectedBSRHashMaskLength
   pimBsrElectedBSRExpiryTime
```
**show ip pim notifications**

Displays the configuration of the configured notification periods as well as information on the events triggering the notifications.

```
show ip pim notifications
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The outputs from this command includes both IPv4 and IPv6 information.

**Examples**

```
--> show ip pim notifications
Neighbor Loss Notifications
   Period  = 0
   Count   = 0
Invalid Register Notifications
   Period  = 65535
   Msgs Rcvd = 0
   Origin   = None
   Group    = None
   RP       = None
Invalid Join Prune Notifications
   Period  = 65535
   Msgs Rcvd = 0
   Origin   = None
   Group    = None
   RP       = None
RP Mapping Notifications
   Period  = 65535
   Count   = 0
Interface Election Notifications
   Period  = 65535
   Count   = 0
```
Non Bidir Hello Notifications

<table>
<thead>
<tr>
<th>Period</th>
<th>65535</th>
</tr>
</thead>
<tbody>
<tr>
<td>Msgs Rcvd</td>
<td>0</td>
</tr>
<tr>
<td>Origin</td>
<td>None</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Loss Notification</td>
<td><strong>Period</strong>: Minimum time interval that must elapse between the PIM neighbor loss notification originated by the device. <strong>Count</strong>: The number of neighbor loss events that have occurred. This counter is incremented whenever a neighbor loss notification is generated.</td>
</tr>
<tr>
<td>Invalid Register Notification</td>
<td><strong>Period</strong>: Minimum time interval that must elapse between the PIM invalid register notifications originated by the device. <strong>Msgs Rcvd</strong>: The number of invalid PIM register notification messages that have been received by the device. <strong>Group</strong>: The multicast group address to which the last unexpected Register message received by the device was addressed. <strong>RP</strong>: The RP address to which the last unexpected Register message received by the device was delivered. <strong>Origin</strong>: The source address of the last unexpected Register message received by the device.</td>
</tr>
<tr>
<td>Invalid Join/Prune Notification</td>
<td><strong>Period</strong>: Minimum time that must elapse between PIM invalid join/prune notifications originated by the device. <strong>Msgs Rcvd</strong>: The number of invalid PIM join/prune messages that have been received by the device. <strong>Origin</strong>: The source address of the last unexpected join/prune message received by the device. <strong>Group</strong>: The multicast group address carried in the last unexpected join/prune message received by the device. <strong>RP</strong>: The RP address carried in the last unexpected join/prune message received by the device.</td>
</tr>
<tr>
<td>RP Mapping Notifications</td>
<td><strong>Period</strong>: Minimum time that must elapse between PIM RP mapping change notifications originated by the device. <strong>Count</strong>: The number of changes to active RP mappings on this device.</td>
</tr>
<tr>
<td>Interface Election Notifications</td>
<td><strong>Period</strong>: Minimum time that must elapse between PIM Interface Election traps originated by the router. <strong>Count</strong>: The number of times this device has been elected DR on any interface.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; **Non Bidir Hello Notifications** field added.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip pim neighbor-loss-notification-period</code></td>
<td>Specifies the minimum time that must elapse between PIM neighbor loss notifications originated by the router.</td>
</tr>
<tr>
<td><code>ip pim invalid-register-notification-period</code></td>
<td>Specifies the minimum time that must elapse between PIM invalid register notifications originated by the router.</td>
</tr>
<tr>
<td><code>ip pim invalid-joinprune-notification-period</code></td>
<td>Specifies the minimum time that must elapse between PIM invalid joinprune notifications originated by the router.</td>
</tr>
<tr>
<td><code>ip pim rp-mapping-notification-period</code></td>
<td>Specifies the minimum time that must elapse between PIM RP mapping notifications originated by this router.</td>
</tr>
<tr>
<td><code>ip pim interface-election-notification-period</code></td>
<td>Specifies the minimum time that must elapse between the PIM interface election notifications originated by the router.</td>
</tr>
<tr>
<td><code>ip pim nonbidir-hello-notification-period</code></td>
<td>Specifies the minimum time that must elapse between notifications that the BIDIR-PIM router has received a PIM Hello message from a router that is not a BIDIR-PIM router.</td>
</tr>
</tbody>
</table>

### MIB Objects

- ALCATEL-IND1-PIM-MIB.mib
  - `alaPimsmGlobalConfig`: Includes:
    - `alaPimsmNonBidirHelloPeriod`
    - `alaPimsmNonBidirHelloMsgsRcvd`
    - `alaPimsmNonBidirHelloOrigin`

- PIM-STD-MIB.mib
  - `pim`: Includes:
    - `pimNeighborLossNotificationPeriod`
    - `pimNeighborLossCount`
    - `pimInvalidRegisterNotificationPeriod`
    - `pimInvalidRegisterMsgsRcvd`
    - `pimInvalidRegisterGroup`
    - `pimInvalidRegisterRp`
    - `pimInvalidJoinPruneNotificationPeriod`
    - `pimInvalidJoinPruneMsgsRcvd`
    - `pimInvalidJoinPruneOrigin`
    - `pimInvalidJoinPruneGroup`
    - `pimInvalidJoinPruneRP`
    - `pimRPMappingNotificationPeriod`
    - `pimRPMappingChangeCount`
    - `pimInterfaceElectionNotificationPeriod`
    - `pimInterfaceElectionWinCount`
**show ip pim groute**

Displays (*,G) routing table entries for IPv4 PIM.

**show ip pim groute [group_address]**

---

**Syntax Definitions**

- **group_address**
  
  A 32-bit multicast address. If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

---

**Defaults**

By default, the entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

When the **group_address** is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

---

**Examples**

```
-> show ip pim groute
Total 1 (*,G)

Group Address RP Address RPF Interface Upstream Neighbor UpTime Mode
-----------------------+-----------------+-----------------+-----------------+------------+-------+-------+-------+
225.0.0.0 212.61.60.8 vlan-30 212.61.30.7 00h:01m:43s asm
225.0.0.1 212.61.60.8 vlan-30 212.61.30.7 00h:01m:43s bidir
```

```
-> show ip pim groute 225.0.0.0
(*,225.0.0.0)
  UpTime = 00h:01m:49s
  RP Address = 212.61.60.8,
  PIM Mode = ASM,
  PIM Mode Origin = BSR,
  Upstream Join State = Joined,
  Upstream Join Timer = 00h:00m:11s,
  Upstream Neighbor = 212.61.30.7,
  RPF Interface = vlan-30,
```
RPF Next Hop            = 212.61.30.7,
RPF Route Protocol      = OSPF,
RPF Route Address       = 212.61.60.0/24,
RPF Route Metric Pref   = 110,
RPF Route Metric        = 2,
Interface Specific State:
  vlan-4
    UpTime                    = 00h:01m:49s,
    Local Membership          = True,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-5
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-8
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-9
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,
  vlan-30
    UpTime                    = 00h:00m:00s,
    Local Membership          = False,
    Join/Prune State          = No Info,
    Prune Pending Timer       = 00h:00m:00s,
    Join Expiry Timer         = 00h:00m:00s,
    Assert State              = No Info,
    Assert Timer              = 00h:00m:00s,

output definitions

<table>
<thead>
<tr>
<th>Group-address</th>
<th>The IPv4 Multicast Group Address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>The address of the Rendezvous Point (RP) for the group.</td>
</tr>
<tr>
<td>RPF Interface</td>
<td>The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.</td>
</tr>
<tr>
<td>Upstream Neighbor</td>
<td>The primary address of the neighbor on the RPF Interface that the local router is sending periodic (*,G) join messages to.</td>
</tr>
<tr>
<td>UpTime</td>
<td>The time since this entry was created.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Whether this entry represents an <code>asm</code> (Any Source Multicast) or <code>bidir</code> (Bidirectional PIM) group.</td>
</tr>
<tr>
<td>Pim Mode Origin</td>
<td>The mechanism by which the PIM mode and RP for the group were learned.</td>
</tr>
<tr>
<td>Upstream Join State</td>
<td>Whether the local router should join the RP tree for the group.</td>
</tr>
<tr>
<td>Upstream Join Timer</td>
<td>The time remaining before the local router next sends a periodic (*,G) Join message on the RPF IfIndex.</td>
</tr>
<tr>
<td>RPF Next Hop</td>
<td>The address of the RPF next hop towards the RP.</td>
</tr>
<tr>
<td>RPF Route Protocol</td>
<td>The routing mechanism through which the route used to find the RPF interface towards the RP was learned.</td>
</tr>
<tr>
<td>RPF Route Address/Prefix Length</td>
<td>The IPv6 address combined with the prefix length identifies the route used to find the RPF interface towards the RP.</td>
</tr>
<tr>
<td>Route Metric Pref</td>
<td>The metric preference of the route used to find the RPF interface towards the RP.</td>
</tr>
<tr>
<td>Route Metric</td>
<td>The routing metric of the route used to find the RPF interface towards the RP.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The interface name that corresponds to the ifIndex.</td>
</tr>
<tr>
<td>Local Membership</td>
<td>Whether the local router has (*,G) local membership on this interface.</td>
</tr>
<tr>
<td>Join Prune State</td>
<td>The state resulting from (*,G) Join/Prune messages received on this interface.</td>
</tr>
<tr>
<td>Prune Pending Timer</td>
<td>The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.</td>
</tr>
<tr>
<td>Join Expiry Timer</td>
<td>The time remaining before (*,G) Join state for this interface expires.</td>
</tr>
<tr>
<td>Assert State</td>
<td>The (*,G) Assert state for this interface. The possible values are No Info, Winner, or Loser.</td>
</tr>
<tr>
<td>Assert Timer</td>
<td>If Assert State is 'Winner', this is the time remaining before the local router next sends a (<em>,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (</em>,G) assert state expires.</td>
</tr>
<tr>
<td>Assert Winner Address</td>
<td>If the Assert State is 'Loser', this is the address of the assert winner.</td>
</tr>
<tr>
<td>Assert Winner Metric Pref</td>
<td>If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.</td>
</tr>
<tr>
<td>Assert Winner Metric</td>
<td>If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; Mode field added, `bidir` mode support added

Related Commands

- **show ip pim sgroute** Displays (S,G) state routing table entries.
MIB Objects

pimStarGTable
   pimStarGAddressType
   pimStarGGrpAddress
   pimStarGUpTime
   pimStarGPimMode
   pimStarGRPAAddressType
   pimStarGRPAAddress
   pimStarGPimModeOrigin
   pimStarGRPIsLocal
   pimStarGUpstreamJoinState
   pimStarGUpstreamJoinTimer
   pimStarGUpstreamNeighborType
   pimStarGUpstreamNeighbor
   pimStarGRPFifIndex
   pimStarGRPFNextHopType
   pimStarGRPFNextHop
   pimStarGRPFRouteProtocol
   pimStarGRPFRouteAddress
   pimStarGRPFRoutePrefixLength
   pimStarGRPFRouteMetric
   pimStarGRPFRouteMetric
pimStarGITable
   pimStarGIfIndex
   pimStarGUpTime
   pimStarGILocalMembership
   pimStarGIJoinPruneState
   pimStarGIPrunePendingTimer
   pimStarGIJoinExpiryTimer
   pimStarGIAssertState
   pimStarGIAssertTimer
   pimStarGIAssertWinnerAddressType
   pimStarGIAssertWinnerAddress
   pimStarGIAssertWinnerMetric
   pimStarGIAssertWinnerMetric
show ip pim sgroute

Displays (S,G) routing table entries for IPv4 PIM.

`show ip pim sgroute [source_address group_address]`

Syntax Definitions

- `source_address`: The 32-bit IP address for a specific multicast source.
- `group_address`: A 32-bit multicast address.

Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the `source_address` and `group_address` associated with that entry.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When the `source_address` and `group_address` is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

Examples

```
-> show ip pim sgroute
Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
        L = Local, R = RPT, T = SPT, F = Register,
        P = Pruned, O = Originator
Total 1 (S,G)

Source Address Group Address RPF Interface Upstream Neighbor UpTime Flags
------------------------------------------------------------------------------------------------------------
172.21.63.2 225.0.0.0 vlan-30 212.61.30.7 00h:02m:09s ST
172.21.63.2 225.0.0.1 vlan-30 212.61.30.7 00h:02m:09s ST

-> show ip pim sgroute 172.21.63.2 225.0.0.0
(172.21.63.2,225.0.0.0)
UpTime = 00h:02m:16s
PIM Mode = ASM,
Upstream Join State = Joined,
Upstream RPT State = Not Pruned,
```

---

**show ip pim sgroute**

Displays (S,G) routing table entries for IPv4 PIM.

**show ip pim sgroute [source_address group_address]**

**Syntax Definitions**

- `source_address`: The 32-bit IP address for a specific multicast source.
- `group_address`: A 32-bit multicast address.

**Defaults**

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the `source_address` and `group_address` associated with that entry.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the `source_address` and `group_address` is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IP address is not specified, the current PIM status for all multicast route entries are displayed.

**Examples**

```
-> show ip pim sgroute
Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
        L = Local, R = RPT, T = SPT, F = Register,
        P = Pruned, O = Originator
Total 1 (S,G)

Source Address Group Address RPF Interface Upstream Neighbor UpTime Flags
------------------------------------------------------------------------------------------------------------
172.21.63.2 225.0.0.0 vlan-30 212.61.30.7 00h:02m:09s ST
172.21.63.2 225.0.0.1 vlan-30 212.61.30.7 00h:02m:09s ST

-> show ip pim sgroute 172.21.63.2 225.0.0.0
(172.21.63.2,225.0.0.0)
UpTime = 00h:02m:16s
PIM Mode = ASM,
Upstream Join State = Joined,
Upstream RPT State = Not Pruned,
```
Upstream Join Timer     = 00h:00m:44s,
Upstream Neighbor       = 212.61.30.7,
RPF Interface           = vlan-30,
RPF Next Hop            = 212.61.30.7,
RPF Route Protocol      = OSPF,
RPF Route Address       = 172.21.63.0/24,
RPF Route Metric Pref   = 110,
RPF Route Metric        = 2,
SPT Bit                 = True,
DR Register State       = No Info,
DR Register Stop Timer  = 00h:00m:00s,
Interface Specific State:
  vlan-4
    UpTime                 = 00h:02m:16s,
    Local Membership       = True,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-5
    UpTime                 = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-8
    UpTime                 = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-9
    UpTime                 = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
  vlan-30
    UpTime                 = 00h:00m:00s,
    Local Membership       = False,
    Join/Prune State       = No Info,
    RPT State              = No Info,
    Prune Pending Timer    = 00h:00m:00s,
    Join Expiry Timer      = 00h:00m:00s,
    Assert State           = No Info,
    Assert Timer           = 00h:00m:00s,
### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-address</td>
<td>The IPv4 Source address.</td>
</tr>
<tr>
<td>Group-address</td>
<td>The IPv4 Multicast Group Address.</td>
</tr>
<tr>
<td>RPF Interface</td>
<td>The RPF interface towards the RP. The ifIndex is converted to the if-name for the display.</td>
</tr>
<tr>
<td>Upstream Neighbor</td>
<td>The primary address of the neighbor on the RPF Interface that the local router is sending periodic (S,G) join messages to.</td>
</tr>
<tr>
<td>UpTime</td>
<td>The time since this entry was created.</td>
</tr>
<tr>
<td>Flags</td>
<td>Flags indicating SPTBit, Prune State, Join State, etc.</td>
</tr>
<tr>
<td>Pim Mode</td>
<td>Whether the Group Address is SSM, ASM or DM.</td>
</tr>
<tr>
<td>Upstream Join State</td>
<td>Whether the local router should join the SPT for the source and group represented by this entry.</td>
</tr>
<tr>
<td>Upstream Join Timer</td>
<td>The time remaining before the local router next sends a periodic (S,G) Join message.</td>
</tr>
<tr>
<td>RPF Next Hop</td>
<td>The address of the RPF next hop towards the source.</td>
</tr>
<tr>
<td>RPF Route Protocol</td>
<td>The routing mechanism through which the route used to find the RPF Interface towards the source was learned.</td>
</tr>
<tr>
<td>RPF Route Address/Prefix Length</td>
<td>The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.</td>
</tr>
<tr>
<td>RPF Route Metric Pref</td>
<td>The metric preference of the route used to find the RPF interface towards the source.</td>
</tr>
<tr>
<td>RPF Route Metric</td>
<td>The metric preference of the route used to find the RPF interface towards the source.</td>
</tr>
<tr>
<td>DR Register State</td>
<td>Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.</td>
</tr>
<tr>
<td>DR Register Stop Timer</td>
<td>The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.</td>
</tr>
<tr>
<td>Upstream Prune State</td>
<td>Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.</td>
</tr>
<tr>
<td>Upstream Prune Limit Timer</td>
<td>The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFIfIndex. This is only used by PIM-DM.</td>
</tr>
<tr>
<td>Originator State</td>
<td>Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.</td>
</tr>
<tr>
<td>Source Active Timer</td>
<td>If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.</td>
</tr>
<tr>
<td>State Refresh Timer</td>
<td>If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>The interface name corresponding to the ifIndex that corresponds to this entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Uptime</strong></td>
<td>The time since this entry was created.</td>
</tr>
<tr>
<td><strong>Local Membership</strong></td>
<td>Whether the local router has (S,G) local membership on this interface.</td>
</tr>
<tr>
<td><strong>Join Prune State</strong></td>
<td>The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.</td>
</tr>
<tr>
<td><strong>Prune Pending Timer</strong></td>
<td>The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.</td>
</tr>
<tr>
<td><strong>Join Expiry Timer</strong></td>
<td>The time remaining before (S,G) Join state for this interface expires.</td>
</tr>
<tr>
<td><strong>Assert State</strong></td>
<td>The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.</td>
</tr>
<tr>
<td><strong>Assert Timer</strong></td>
<td>If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.</td>
</tr>
<tr>
<td><strong>Assert Winner</strong></td>
<td>If the Assert State is Loser, this is the address of the assert winner.</td>
</tr>
<tr>
<td><strong>Assert Winner Metric Pref</strong></td>
<td>If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.</td>
</tr>
<tr>
<td><strong>Assert Winner Metric Metric</strong></td>
<td>If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show ip pim groute** Displays (*,G) routing table entries for IPv4 PIM.
**MIB Objects**

```
pimSGTable
    pimSGAddressType
    pimSGGrpAddress
    pimSGSrcAddress
    pimGUptime
    pimGPimMode
    pimGUptstreamJoinState
    pimGUptstreamJoinTimer
    pimGUptstreamNeighbor
    pimGSRPF InterfaceIndex
    pimGSRPF NextHopType
    pimGSRPF NextHop
    pimGSRPF RouteProtocol
    pimGSRPF RouteAddress
    pimGSRPF RoutePrefixLength
    pimGSRPF RouteMetricPref
    pimGSRPF RouteMetric
    pimGSPtreeBit
    pimGKeepalive Timer
    pimGDRRegister State
    pimGDRRegister Stop Timer
    pimGDRPFRegister FMBR Address Type
    pimGDRPFRegister FMBR Address
    pimGUptstream Prune State
    pimGUptstream Prune Limit Timer
    pimGOriginator State
    pimGSSource Active Timer
    pimGSSource Refresh Timer

pimSGITable
    pimGIIInterfaceIndex
    pimGIIUpTime
    pimGII Local Membership
    pimGIIJoin Prune State
    pimGII Prune Pending Timer
    pimGII Join Expiry Timer
    pimGII Assert State
    pimGII Assert Timer
    pimGII Assert Winner Address Type
    pimGII Assert Winner Address
    pimGII Assert Winner Metric Pref
    pimGII Assert Winner Metric
```
show ip pim df-election

Displays the Designated Forwarder (DF) election state for Rendezvous Point (RP) interfaces. This command applies only to RPs operating in the Bidirectional PIM (BIDIR-PIM) mode.

**show ip pim df-election [rp_address | if_name]**

### Syntax Definitions

- **rp_address**: A 32-bit RP address.
- **if_name**: The interface name.

### Defaults

By default, the DF election state for all RP interfaces.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When the **rp_address** is specified in the command line, only those interfaces associated with the specified RP address are displayed.
- When the **if_name** is specified in the command line, only information associated with the specified interface is displayed.

### Examples

```
-> show ip pim df-election
RP Address Interface Name DF State Winner Address Uptime Metric Metric Expires Pref
---------------------------------------------------------------
10.11.203.8 vlan-13 Win 10.11.126.3 00h:06m:31s 1 1 00h:00m:24s
vlan-200 Win 10.11.200.1 00h:06m:31s 1 1 00h:00m:24s
vlan-204 Win 10.11.204.8 00h:06m:31s 1 1 00h:00m:24s
vlan-210 Win 10.5.5.8 00h:06m:31s 1 1 00h:00m:24s
40.1.50.25 vlan-203 Lose 10.11.203.27 00h:00m:22s 1 1 00h:00m:00s
vlan-13 Win 10.11.126.3 00h:06m:31s 110 2 00h:00m:32s
vlan-200 Win 10.11.200.1 00h:06m:31s 110 2 00h:00m:32s
vlan-204 Lose 10.11.204.27 00h:00m:22s 1 1 00h:00m:00s
vlan-210 Win 10.5.5.8 00h:06m:31s 110 2 00h:00m:32s

-> show ip pim df-election 40.1.50.25
RP Address Interface Name DF State Winner Address Uptime Metric Metric Expires Pref
---------------------------------------------------------------
```

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 34-131
PIM Commands

---

show ip pim df-election

<table>
<thead>
<tr>
<th>RP Address</th>
<th>Interface Name</th>
<th>DF State</th>
<th>Winner Address</th>
<th>Uptime</th>
<th>Metric</th>
<th>Metric Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>40.1.50.25</td>
<td>vlan-203</td>
<td>Lose</td>
<td>10.11.203.27</td>
<td>00h:00m:22s 1</td>
<td>1</td>
<td>00h:00m:00s</td>
</tr>
<tr>
<td>vlan-13</td>
<td>Win</td>
<td></td>
<td>10.11.126.3</td>
<td>00h:06m:31s 110</td>
<td>2</td>
<td>00h:00m:32s</td>
</tr>
<tr>
<td>vlan-200</td>
<td>Win</td>
<td></td>
<td>10.11.200.1</td>
<td>00h:06m:31s 110</td>
<td>2</td>
<td>00h:00m:32s</td>
</tr>
<tr>
<td>vlan-204</td>
<td>Lose</td>
<td></td>
<td>10.11.204.27</td>
<td>00h:00m:22s 1</td>
<td>1</td>
<td>00h:00m:00s</td>
</tr>
<tr>
<td>vlan-210</td>
<td>Win</td>
<td></td>
<td>10.5.5.8</td>
<td>00h:06m:31s 110</td>
<td>2</td>
<td>00h:00m:32s</td>
</tr>
</tbody>
</table>

-> show ip pim df-election vlan-200

<table>
<thead>
<tr>
<th>RP Address</th>
<th>Interface Name</th>
<th>DF State</th>
<th>Winner Address</th>
<th>Uptime</th>
<th>Metric</th>
<th>Metric Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.11.203.8</td>
<td>vlan-200</td>
<td>Win</td>
<td>10.11.200.1</td>
<td>00h:06m:31s 1</td>
<td>1</td>
<td>00h:00m:24s</td>
</tr>
<tr>
<td>40.1.50.25</td>
<td>vlan-200</td>
<td>Win</td>
<td>10.11.200.1</td>
<td>00h:06m:31s 110</td>
<td>2</td>
<td>00h:00m:32s</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>RP Address</th>
<th>Interface Name</th>
<th>DF State</th>
<th>Winner Address</th>
<th>UpTime</th>
<th>Metric</th>
<th>Metric Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IPv4 address of the Rendezvous Point (RP).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The name of the IPv4 interface.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The state of the DF election process (Offer, Lose, Win, or Backoff).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The primary IPv4 address of the winner of the DF election process.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The amount of time since the current winner was last elected the DF for the RP.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The metric preference advertised by the DF winner. This value is zero if there currently is no DF.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The metric value advertised by the DF winner. This value is zero if there currently is no DF.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The minimum time remaining before the local router expires the current DF state.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

*show ip pim interface* Displays detailed PIM settings for a specific interface.

**MIB Objects**

* pimBidirDFElectionTable
  * pimBidirDFElectionAddressType
  * pimBidirDFElectionRPAddress
  * pimBidirDFElectionIfIndex
  * pimBidirDFElectionWinnerAddressType
  * pimBidirDFElectionWinnerAddress
  * pimBidirDFElectionWinnerUpTime
  * pimBidirDFElectionWinnerMetricPref
  * pimBidirDFElectionWinnerMetric
  * pimBidirDFElectionState
  * pimBidirDFElectionStateTimer
**ipv6 pim sparse admin-state**

Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.

`ipv6 pim sparse admin-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables PIM-SM globally for IPv6.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables PIM-SM globally for IPv6.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command must be set to `enable` before PIM-SM can run on the switch. In addition, the `ip load pim` command must be executed. Refer to page 34-3 for more information.

**Examples**

- `-> ipv6 pim sparse admin-state enable`
- `-> ipv6 pim sparse admin-state disable`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ipv6 pim interface**
  Enables or disables the PIM protocol on a specific interface.

- **ip load pim**
  Dynamically loads PIM to memory.

- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

**MIB Objects**

- `alaPimsmGlobalConfig`
- `alaPimsmV6AdminStatus`
ipv6 pim bidir admin-state

Enables or disables IPv6 BIDIR-PIM (bidirectional) globally for IPv6.

ipv6 pim bidir admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables BIDIR-PIM globally for IPv6.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables BIDIR-PIM globally for IPv6.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command must be set to enable before BIDIR-PIM can run on the switch. In addition, the ip load pim command must be executed. Refer to page 34-3 for more information.

Examples

-> ipv6 pim bidir admin-state enable
-> ipv6 pim bidir admin-state disable

Release History

Release 7.3.4; command was introduced.
Related Commands

- **ipv6 pim interface**
  Enables or disables the PIM protocol on a specific interface.
- **ip load pim**
  Dynamically loads PIM to memory.
- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

- **alaPimsmGlobalConfig**
- **alaPimsmV6BidirStatus**
**ipv6 pim dense admin-state**

Enables or disables the IPv6 PIM-DM (dense mode) globally for IPv6.

```
ipv6 pim dense admin-state {enable | disable}
```

### Syntax Definitions

- **enable**: Enables PIM-DM globally for IPv6.
- **disable**: Disables PIM-DM globally for IPv6.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command must be set to **enable** before PIM-DM can run on the switch. In addition, the **ip load pim** command must be executed. Refer to page 34-3 for more information.

### Examples

```
-> ipv6 pim dense admin-state enable
-> ipv6 pim dense admin-state disable
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- `ipv6 pim interface` Enables or disables the PIM protocol on a specific interface.
- `ip load pim` Dynamically loads PIM to memory.
- `show ipv6 pim dense` Displays the status of the various global parameters for the IPv6 PIM dense mode.

**MIB Objects**

- `alaPimdmGlobalConfig`
- `alaPimdmV6AdminStatus`
**ipv6 pim ssm group**

Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

```
ipv6 pim ssm group group_address/prefix_length [[no] override] [priority priority]
no ipv6 pim ssm group group_address/prefix_length
```

### Syntax Definitions

- `group_address` Specifies the IPv6 multicast group address.
- `/prefix_length` Specifies the prefix length of the IPv6 multicast group. Values may range from 4 to 128.
- `override` Specifies the static SSM mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
- `priority` Specifies the preference value to be used for this static SSM mode configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

### Defaults

By default, the priority option is not set and the override option is set to false.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove a static configuration of a Source Specific Multicast mode group mapping.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be configured manually to support SSM.
- You can also map additional IPv6 multicast address ranges for the SSM group using this command. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
• Specifying the priority value obsoletes the `override` option and once the priority option has been defined, a value of 65535 can be used to unset the priority.

**Examples**

```plaintext
-> ipv6 pim ssm group ff30::1234:abcd/128 priority 50
-> no ipv6 pim ssm group ff30::1234:abcd/128
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 pim group-map</code></td>
<td>Displays the IPv6 PIM group mapping table.</td>
</tr>
<tr>
<td><code>show ipv6 pim ssm group</code></td>
<td>Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).</td>
</tr>
</tbody>
</table>

**MIB Objects**

```plaintext
pimStaticRPTable
   pimStaticRPGrpAddress
   pimStaticRPGrpPrefixLength
   pimStaticRPImMode
   pimStaticRPPrecedence
   pimStaticRPOccerideDynamic
   pimStaticRPRowStatus
```
ipv6 pim dense group

Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

`ipv6 pim dense group group_address/prefix_length [no] override] [priority priority]

no ipv6 pim dense group group_address/prefix_length`

**Syntax Definitions**

- `group_address` Specifies the IPv6 multicast group address.
- `/prefix_length` Specifies the prefix length of the IPv6 multicast group.
- `override` Specifies the static dense mode mapping configuration to override the dynamically learned group mapping information for the specified group(s).
- `priority` Specifies the preference value to be used for this static configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

**Defaults**

By default, the priority option is not set and the override option is set to false.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a static configuration of a dense mode group mapping.
- This command specifies the mode as Dense (PIM-DM) for the specified IPv6 multicast group addresses.
- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.
- Specifying the priority value obsoletes the `override` option and once the priority option has been defined, a value of 65535 can be used to unset the priority.

**Examples**

- `-> ipv6 pim dense group ff0e::1234/128 priority 50`
- `-> no ipv6 pim dense group ff0e::1234/128`
Release History

Release 7.1.1; command was introduced.

Related Commands

show ipv6 pim group-map  Displays the IPv6 PIM group mapping table.
show ipv6 pim dense group Displays the static configuration of IPv6 multicast group mappings
                  for PIM Dense Mode (DM).

MIB Objects

alaPimdmDenseGroupTable
    alaPimdmDenseGroupGrpAddress
    alaPimdmDenseGroupGrpPrefixLength
    alaPimdmDenseGroupOverrideDynamic
    alaPimdmDenseGroupPrecedence
    alaPimdmDenseGroupRowStatus
**ipv6 pim cbsr**

Configures the local router as the Candidate-BSR for the PIM domain.

```
ipv6 pim cbsr ipv6_address [priority priority] [mask-length bits]
```

```
no ipv6 pim cbsr ipv6_address
```

### Syntax Definitions

- **ipv6_address**: The IPv6 unicast address that the local router will use to advertise itself as a Candidate-BSR. The specified address must be a domain-wide reachable address.

- **priority**: The priority value of the local router as a Candidate-BSR. Values may range from 0 to 255.

- **bits**: The hash mask length that is advertised in the bootstrap messages for IPv6 PIM (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group). Values may range from 1 to 128.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>64</td>
</tr>
<tr>
<td>bits</td>
<td>126</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the association of the device as a Candidate-BSR for a PIM domain.

- This command is supported only in the sparse mode.

- The information configured using this command is used in the Bootstrap messages.

- Candidate-BSRs also avoid a single point of failure in a PIM domain.

### Examples

```
-> ipv6 pim cbsr 2000::1 priority 100 mask-length 4
```
-> no ipv6 pim cbsr 2000::1

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ipv6 pim cbsr` Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages.

**MIB Objects**

- `pimBsrCandidateBSRTable`
  - `pimBsrCandidateBSRAddress`
  - `pimBsrCandidateBSRPriority`
  - `pimBsrCandidateBSRHashMaskLength`
  - `pimBsrCandidateBSRRowStatus`
**ipv6 pim static-rp**

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

```
ipv6 pim static-rp group_address/prefix_length rp_address [no] bidir [no] override [priority priority]
```

```
no ipv6 pim static-rp group_address/prefix_length rp_address
```

**Syntax Definitions**

- `group_address`: Specifies the IPv6 multicast group address.
- `/prefix_length`: Specifies the prefix length of the IPv6 multicast group.
- `rp_address`: Specifies the IPv6 unicast address of the Rendezvous Point (RP). This must be a domain-wide reachable address.
- `bidir`: Creates the static RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.
- `override`: Specifies the static RP configuration to override the dynamically learned RP information for the specified group(s).
- `priority`: Specifies the preference value to be used for this static RP configuration and provides fine control over which configuration is overridden by this static configuration. Values may range from 0 to 128.

**Defaults**

By default, the `priority` option is not set, the `override` option is set to false, and the `bidir` option is set to false.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete a static RP configuration.
- Specifying the priority value obsoletes the `override` option.
- If the `bidir` parameter option is not specified with this command, the static RP entry is created for use in the ASM mode.
- The IPv6 PIM Source-Specific Multicast (SSM) mode for the default SSM address range (FF3x::/32) reserved by the Internet Assigned Numbers Authority is not enabled automatically and must be
configured manually to support SSM. You can also map additional IPv6 multicast address ranges for the SSM group. However, the IPv6 multicast groups in the reserved address range can be mapped only to the SSM mode.

- If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range
- Note that once the priority option has been defined a value of 65535 can be used to unset the priority
- This command is supported only in the sparse mode.

**Examples**

```
-> ipv6 pim static-rp ff0e::1234/128 2000::1 priority 10
-> ipv6 pim static-rp ff0e::1234/128 2000::1 bidir override
-> no ipv6 pim static-rp ff0e::1234/128 2000::1
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; bidir parameter added.

**Related Commands**

- `show ipv6 pim group-map` Displays the IPv6 PIM group mapping table.
- `show ipv6 pim static-rp` Displays the IPv6 PIM Static RP table, which includes IPv6 multicast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the Static RP configuration (i.e., enabled or disabled).

**MIB Objects**

- `pimStaticRPTable`  
  `pimStaticRPGrpAddress`
  `pimStaticRPGrpPrefixLength`
  `pimStaticRPRPAddress`
  `pimStaticRPImMode`
  `pimStaticRPOverrideDynamic`
  `pimStaticRPPrecedence`
  `pimStaticRPRowStatus`
ipv6 pim anycast-rp

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

ipv6 pim anycast-rp anycast_rp_address rp_address

no ipv6 pim anycast-rp anycast_rp_address rp_address

Syntax Definitions

anycast-rp-address Specifies the anycast RP address.

rp_address Specifies the IPv6 unicast address of the Rendezvous Point (RP) address of a router that is a member of the anycast RP set.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to delete an anycast RP configuration.

- The RP specified by anycast-RP-address is the RP in the anycast RP set. This address must be the same as the RP address in the Static-RP configuration used with the *ipv6 pim static-rp* command if static RP configuration is being used.

- It is recommended not to use Loopback0 as the anycast RP address since Loopback0 is often used as the Router ID by default with the unicast routing protocols. Hence, it is recommended to use one of the additional LoopbackX interfaces for the anycast RP address, but it is not mandatory to be a LoopbackX address.

- The RP specified by rp-address defines the IP address of the prospective RP. This address must be different than the anycast RP address and is used in communication between the different RPs in the anycast RP set. This configuration must be the same on all routers in the Anycast-RP set.

- There must be a separate entry for each of the RPs participating in anycast RP set, including an entry for the local router. This configuration defining the anycast RP set must be the same on all routers participating in anycast RP.

- It is recommended to configure PIM register rate limiting (see *ipv6 pim register-rate-limit*) to limit the sending of PIM register messages with Anycast RP.
• Ensure SPT is enabled (see `ipv6 pim spt admin-state`) when using Anycast RP. If SPT is globally disabled, and Anycast RP configuration is added, this configuration will be ignored for all groups that are operating in Anycast-RP mode.

**Examples**

-> `ipv6 pim static-rp ff00::/8 2001:1::1`
-> `ipv6 pim anycast-rp 2001:1::1 3001:1::1`
-> `ipv6 pim anycast-rp 2001:1::1 3001:1::2`
-> `no ipv6 pim anycast-rp 2001:1::1 3001:1::2`

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

**ipv6 pim static-rp**

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

**show ipv6 pim anycast-rp**

Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration.

**MIB Objects**

`pimAnycastRPSetTable`

- `pimAnycastRPSetAddressType`
- `pimAnycastRPSetAddressAnycastAddress`
- `pimAnycastRPSetAddressRouterAddress`
- `pimAnycastRPSetAddressRowStatus`
ipv6 pim candidate-rp

Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s). This command is supported only in the sparse mode.

`ipv6 pim candidate-rp rp_address group_address/prefix_length [no bidir] [priority priority] [interval seconds]`

`no ipv6 pim candidate-rp rp_address group_address/prefix_length`

### Syntax Definitions

- **rp_address**
  Specifies the IPv6 unicast address that will be advertised as a Candidate-RP. This must be a domain-wide reachable address.

- **group_address**
  Specifies the IPv6 multicast group address for which the local router will advertise itself as a Candidate-RP.

- **/prefix_length**
  Specifies the prefix length of the specified IPv6 multicast group address.

- **bidir**
  Creates a C-RP entry for use in the Bidirectional PIM (BIDIR-PIM) mode.

- **priority**
  Specifies the priority value of the Candidate-RP. Values may range from 0 to 192. The lower the value, the higher the priority.

- **seconds**
  Specifies the interval at which the C-RP advertisements are sent to the bootstrap router, in seconds. Values may range from 1 to 300.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] bidir</td>
<td>no bidir</td>
</tr>
<tr>
<td>priority</td>
<td>192</td>
</tr>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the association of the device as a C-RP for a particular multicast group.
- Only one RP address is supported per switch. If multiple candidate-RP entries are defined, they must specify the same `rp-address`. 
• If the `bidir` parameter option is not specified with this command, the C-RP entry is created for use in the ASM mode.

**Examples**

```
-> ipv6 pim candidate-rp 2000::1 ff0e::1234/128 priority 100 interval 100
-> ipv6 pim candidate-rp 2000::1 ff0e::1234/128 bidir priority 100 interval 100
-> no ipv6 pim candidate-rp 2000::1 ff0e::1234/128
```

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; `bidir` parameter added.

**Related Commands**

`show ipv6 pim candidate-rp` Displays the IPv6 multicast groups for which the local router will advertise itself as a Candidate-RP.

**MIB Objects**

`pimBsrCandidateRPTable`

`pimBsrCandidateRPAAddress`
`pimBsrCandidateRPGroupAddress`
`pimBsrCandidateRPGroupPrefixLength`
`pimBsrCandidateRPBidir`
`pimBsrCandidateRPPriority`
`pimBsrCandidateRPAdvInterval`
`pimBsrCandidateRPRowStatus`
ipv6 pim rp-switchover

Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain. This command is supported only in the sparse mode.

ipv6 pim rp-switchover {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables the RP to switch to native forwarding.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables the RP from switching to native forwarding.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

You cannot specify a pre-configured threshold, such as the RP threshold, as you would do for IPv4 PIM.

Examples

`-> ipv6 pim rp-switchover enable`

`-> ipv6 pim rp-switchover disable`

Release History

Release 7.1.1; command was introduced.
**Related Commands**

**show ipv6 pim sparse**  
Displays the status of the various global parameters for the IPv6 PIM sparse mode.

**MIB Objects**

alaPimsmGlobalConfig

alaPimsmV6RPSwitchover
**ipv6 pim register-rate-limit**

Configures the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry. This command is supported only in the sparse mode.

```plaintext
ipv6 pim register-rate-limit pps
```

---

**Syntax Definitions**

`pps` The per (S,G) register rate limit in packets per second (0–65535).

---

**Defaults**

By default, the register rate limit is set to zero.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Setting the register rate limit to zero (the default) disables register rate limiting.
- Rate limiting is applied on a per (S,G) flow basis.
- This command is supported in both IPv4 and IPv6 PIM.

---

**Examples**

```plaintext
-> ipv6 pim register-rate-limit 100
-> ipv6 pim register-rate-limit 0
```

---

**Release History**

Release 8.4.1.R02; command was introduced.
**Related Commands**

- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

- **show ip pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

**MIB Objects**

- aLaPimsmGlobalConfigTable
  - aLaPimsmV6RegisterRateLimit
**ipv6 pim register-packing**

Enables or disables the PIM Register Message Packing.

`ipv6 pim register-packing {enable | disable | force-enable}`

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the PIM register packing.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the PIM register packing.</td>
</tr>
<tr>
<td>force-enable</td>
<td>Force enables the PIM register packing</td>
</tr>
</tbody>
</table>

### Defaults

By default, PIM register packing is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When using this command with Anycast-RP, PIM register packing should be enabled only if it is supported by all PIM anycast RP members in the RP set for the RP address.

- It is recommended to use the configuration value of "force-enable" on all the routers in the domain, when register message packing is desired and Anycast-RP is used.

- When the value “force-enable” is used, the null registers will automatically be packed without waiting for acknowledgment from an RP on whether or not the packing of register messages is supported.

- This command is supported only in the sparse mode.

### Examples

- `ipv6 pim register-packing enable`
- `ipv6 pim register-packing force-enable`
- `ipv6 pim register-packing disable`

### Release History

Release 8.7R2; command was introduced.
**Related Commands**

- `show ipv6 pim sparse` Displays the status of the various global parameters for the PIM sparse mode.
- `ipv6 pim register-mtu` Configures the maximum size of messages used for PIM packed register messages.
- `ipv6 pim register-delay` Configures the Triggered Register Delay interval in milliseconds.

**MIB Objects**

- `alaPimsmGlobalConfig`
- `alaPimsmV6RegisterMsgPackingStatus`
**ipv6 pim register-mtu**

Configures the maximum size of messages used for PIM packed register messages.

```
ipv6 pim register-mtu num
```

### Syntax Definitions

- **num**: Specify the maximum MTU size of the PIM packed register messages in bytes.

### Defaults

By default, the value is 1500.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Before using this command, enable or force-enable PIM register packing by using the `ipv6 pim register-packing` command.
- Use this command to configure the maximum MTU size of packed PIM register messages sent out.
- If the MTU size of the packet is larger than the interface that is used to send the packed messages, those packets may be dropped.
- It is not recommended to configure to a large value unless it is known that all the RP routers in the domain can support the MTU size in order to avoid any fragmentation and reassembly of the packets.
- This command is supported only in the sparse mode.

### Examples

```
-> ipv6 pim register-mtu 1000
```

### Release History

Release 8.7R2; command was introduced.
**Related Commands**

- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the PIM sparse mode.

- **ipv6 pim register-packing**
  Enables or disables the PIM Register Message Packing.

- **ipv6 pim register-delay**
  Configures the Triggered Register Delay interval in milliseconds.

**MIB Objects**

- **alaPimsmGlobalConfig**
- **alaPimsmV6PackedRegisterMsgMtu**
### ipv6 pim register-delay

Configures the Triggered Register Delay interval in milliseconds.

```
ipv6 pim register-delay <num>
```

#### Syntax Definitions

- `num` Specify the Triggered Register Delay interval in milliseconds.

#### Defaults

By default, the value is “0”.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- Before using this command, enable or force-enable PIM register packing by using the `ipv6 pim register-packing` command.

- Use this command to configure the Triggered Register Delay interval in milliseconds and to control the packing of initial bursts of triggered Null Register messages.

- This command is supported only in the sparse mode.

#### Examples

```
-> ipv6 pim register-delay 100
```

#### Release History

Release 8.7R2; command was introduced.
**Related Commands**

- `show ipv6 pim sparse` Displays the status of the various global parameters for the PIM sparse mode.
- `ipv6 pim register-packing` Enables or disables the PIM Register Message Packing.
- `ipv6 pim register-mtu` Configures the maximum size of messages used for PIM packed register messages.

**MIB Objects**

- `alaPimsmGlobalConfig`  
  `alaPimsmV6PackedRegisterMsgDelay`
ipv6 pim spt admin-state

Enables or disables last hop Designated Router (DR) switching to the Shortest Path Tree (SPT). This command is supported only in the sparse mode.

ipv6 pim spt admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables last hop DR switching to the SPT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables last hop DR switching to the SPT.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the SPT status is enabled, last hop DR switching to the SPT begins once the first data packet is received.

Examples

- `ipv6 pim spt admin-state enable`
- `ipv6 pim spt admin-state disable`

Release History

Release 7.1.1; command was introduced.
Related Commands

show ipv6 pim sparse  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

alaPimsmGlobalConfig
alaPimsmV6SPTConfig
ipv6 pim interface

Enables IPv6 PIM and configures the statistics such as hello-interval, triggered-hello, hello-holdtime, join/prune, prune-delay, override-interval, dr-priority, stub interface, prune limit interval, and graft retry interval on the IPv6 interface.

ipv6 pim interface if_name
   [hello-interval seconds]
   [triggered-hello seconds]
   [joinprune-interval seconds]
   [hello-holdtime seconds]
   [joinprune-holdtime seconds]
   [prune-delay milliseconds]
   [override-interval milliseconds]
   [dr-priority priority]
   [prune-limit-interval seconds]
   [graft-retry-interval seconds]
   [df-election-robustness messages]
   [[no] stub]
   [joinprune-mtu bytes]
   [joinprune-delay milliseconds]

no ipv6 pim interface if_name

Syntax Definitions

if_name
   The interface name on which the IPv6 PIM is being enabled or disabled.

hello-interval seconds
   The frequency at which IPv6 PIM Hello messages are transmitted on
   this interface, in seconds. Values may range from 0 to 18000.

triggered-hello seconds
   Specifies the maximum time, in seconds, before a triggered IPv6 PIM
   Hello message is sent on this interface. Values may range from 0 to 60.

joinprune-interval seconds
   The frequency at which periodic IPv6 PIM Join/Prune messages are sent
   on this interface, in seconds. Values may range from 0 to 18000.

hello-holdtime seconds
   Specifies the value of the IPv6 PIM hello-holdtime for this interface.
   This value is set in the Holdtime field of IPv6 PIM Hello messages sent
   on this interface, in seconds. Values may range from 0 to 65535.

joinprune-holdtime seconds
   Specifies the value that is set in the Holdtime field of the IPv6 PIM
   Join/prune messages sent on this interface, in seconds. Values may range
   from 0 to 65535.

prune-delay milliseconds
   Specifies the value of the expected propagation delay between IPv6 PIM
   routers on this network, inserted into the LAN prune-delay option of the
   IPv6 PIM Hello messages sent on this interface, in milliseconds. Values
   may range from 0 to 32767.

override-interval milliseconds
   Specifies the value set in the Override Interval field of the LAN prune-
   delay option of the IPv6 PIM Hello messages sent on this interface, if
   the prune-delay status is enabled, in milliseconds. Values may range
   from 0 to 65535.
**dr-priority** *priority*

Specifies the Designated Router priority set in the DR priority option on this interface. The DR priority option value (1–192). A higher numeric value denotes a higher priority.

**prune-limit-interval** *seconds*

Specifies the minimum interval that must elapse between two successive IPv6 PIM prune messages sent on this interface, in seconds. Values may range from 0 to 65535.

**graft-retry-interval** *seconds*

Specifies the minimum interval that must elapse between two successive IPv6 PIM graft messages sent on this interface, in seconds. Values may range from 0 to 65535.

**df-election-robustness** *messages*

The minimum number of DF-Election messages that must be lost in order for the DF Election to fail on the specified interface. Values may range from 1–65535. This value is used only by BIDIR-PIM.

**stub**

Specifies the interface not to send any IPv6 PIM packets through this interface, and to ignore received IPv6 PIM packets.

**joinprune-mtu** *bytes*

Specifies the maximum size used for PIM Join/Prune packets getting sent out this interface. Values may range from 0 to 9198.

**joinprune-delay** *milliseconds*

Specifies the Join/Prune delay interval in milliseconds. Values may range from 0 to 32767.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hello-interval</strong> <em>seconds</em></td>
<td>30</td>
</tr>
<tr>
<td><strong>triggered-hello</strong> <em>seconds</em></td>
<td>5</td>
</tr>
<tr>
<td><strong>joinprune-interval</strong> <em>seconds</em></td>
<td>60</td>
</tr>
<tr>
<td><strong>hello-holdtime</strong> <em>seconds</em></td>
<td>105</td>
</tr>
<tr>
<td><strong>joinprune-holdtime</strong> <em>seconds</em></td>
<td>210</td>
</tr>
<tr>
<td><strong>prune-delay</strong> <em>milliseconds</em></td>
<td>500</td>
</tr>
<tr>
<td><strong>override-interval</strong> <em>milliseconds</em></td>
<td>2500</td>
</tr>
<tr>
<td><strong>dr-priority</strong> <em>priority</em></td>
<td>1</td>
</tr>
<tr>
<td><strong>prune-limit-interval</strong> <em>seconds</em></td>
<td>60</td>
</tr>
<tr>
<td><strong>graft-retry-interval</strong> <em>seconds</em></td>
<td>3</td>
</tr>
<tr>
<td><strong>df-election-robustness</strong> <em>messages</em></td>
<td>3</td>
</tr>
<tr>
<td><strong>stub</strong></td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>joinprune-mtu</strong> <em>bytes</em></td>
<td>0</td>
</tr>
<tr>
<td><strong>joinprune-delay</strong> <em>milliseconds</em></td>
<td>0</td>
</tr>
</tbody>
</table>
### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to delete an IPv6 PIM interface.

- IPv6 PIM must be enabled globally on the switch before IPv6 PIM will begin running on the interface. To globally enable or disable IPv6 PIM-SM on the switch, refer to the `ipv6 pim sparse admin-state` command on page 34-133. To enable or disable IPv6 PIM-DM on the switch, refer to the `ipv6 pim dense admin-state` command on page 34-137.

- Specifying zero for IPv6 PIM hello-interval represents an infinite time, in which case the periodic IPv6 PIM hello messages are not sent.

- Specifying zero for IPv6 PIM joinprune-interval represents an infinite time, in which case the periodic IPv6 PIM joinprune messages are not sent.

- Specifying the value of 65535 for IPv6 PIM hello-holdtime represents an infinite time. If an IPv6 PIM router gets IPv6 PIM Hello packet from a neighbor with its hello-holdtime value as infinite time, then the router will not time out the sender (neighbor). It is recommended that you use an IPv6 PIM hello-holdtime interval that is 3.5 times the value of the IPv6 PIM hello-interval, or 65535 seconds if the IPv6 PIM hello-interval is set to zero.

- Specifying the value of 65535 for IPv6 PIM joinprune-holdtime represents an infinite time. The receipt of IPv6 Join/Prune messages with its joinprune-holdtime value as infinite time, then this specifies an infinite holdtime for the particular IPv6 join/prune message. It is recommended that you use a joinprune-holdtime interval that is 3.5 times the value of the IPv6 PIM Join/Prune interval defined for the interface, or 65535 seconds if the IPv6 PIM joinprune-interval is set to zero.

- The interface configured as a stub will not send any IPv6 PIM packets through that interface, and any received IPv6 PIM packets are also ignored. By default, an IPv6 PIM interface is not set to be a stub.

- The IPv6 PIM `graft-retry-interval` and `prune-limit-interval` options can be used only with the IPv6 PIM-DM mode.

- If the IPv6 interface on which PIM is enabled is bound to an SPB service, then PIM can operate over an SPB L3 VPN in-line routing configuration (supported only on the OmniSwitch 9900).

- By default, `joinprune-mtu` value is ‘0’ and the configured interface MTU value will be used in determining the maximum packet size that can be used in sending the packed messages. However, if the Join/Prune MTU configuration is specified, the actual maximum size used for PIM Join/Prune messages will be the smaller of the IP MTU value of the interface and the configured interface Join/Prune MTU value.

- The `joinprune-delay` interval is used to delay the sending of triggered Join/Prune messages and may be desirable to allow the packing of triggered Join/Prune messages due to bursts of protocol messages, which may result in subsequent bursts of triggered Join/Prune packets. The default value of ‘0’ implies no deferred processing and will result in no packing of triggered Join/Prune packets.
**Examples**

-> ipv6 pim interface vlan-2 hello-interval 100 triggered-hello 10 joinprune-interval 100 hello-holdtime 350 joinprune-holdtime 400
-> no ipv6 pim interface vlan-2

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4: `df-election robustness` parameter added.
Release 8.6R1; `joinprune-mtu, joinprune-delay` parameters added.

**Related Command**

`show ipv6 pim interface` Displays detailed IPv6 PIM settings for a specific interface.

**MIB Objects**

- `pimInterfaceTable`
  - `pimInterfaceIfIndex`
  - `pimInterfaceStatus`
  - `pimInterfaceHelloInterval`
  - `pimInterfaceTrigHelloInterval`
  - `pimInterfaceJoinPruneInterval`
  - `pimInterfaceHelloHoldtime`
  - `pimInterfaceJoinPruneHoldtime`
  - `pimInterfaceDFElectionRobustness`
  - `pimInterfacePropagationDelay`
  - `pimInterfaceOverrideInterval`
  - `pimInterfaceDRPriority`
  - `pimInterfaceStubInterface`
  - `pimInterfacePruneLimitInterval`
  - `pimInterfaceGraftRetryInterval`

- `alaPimInterfaceAugTable`
  - `alaPimInterfaceJoinPruneDelay`
  - `alaPimInterfaceJoinPruneMtu`
ipv6 pim bfd-state

Enables or disables the registration of IPv6 PIM with the BFD protocol.

ipv6 pim bfd-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables BFD for IPv6 PIM.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables BFD for IPv6 PIM.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/E48C8/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 C32E/T24C2/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- BFD must be globally enabled for the switch and PIM must be registered with BFD at the protocol level before PIM can interact with BFD.
- All the status changes on the neighbors are received from the BFD level and PIM acts based upon the BFD message.
- Whenever a neighbor goes down, PIM will inform BFD to remove that neighbor from the BFD active list.

Examples

Globally enables the BFD protocol for the switch:

```
-> ip bfd admin-state enable
```

Enables and disables the registration of IPv6 PIM with the BFD protocol:

```
-> ipv6 pim bfd-state enable
-> ipv6 pim bfd-state disable
```

Release History

Release 8.4.1.R03; command was introduced.
**Related Commands**

- `ip bfd admin-state` Enables or disables the global BFD protocol status for the switch.
- `ipv6 pim bfd-state all-interfaces` Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.
- `ipv6 pim interface bfd-state` Enables or disables BFD monitoring on a specific PIM interface.
- `show ipv6 pim sparse` Displays the status of the various global parameters for the PIM sparse mode.
- `show ipv6 pim dense` Displays the status of the various global parameters for the PIM dense mode.

**MIB Objects**

- `alaPimGlobal`
- `alaPimBfdStatus`
ipv6 pim bfd-state all-interfaces

Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.

ipv6 pim bfd-state all-interfaces {enable | disable}

Syntax Definitions

enable  Enables BFD for all the IPv6 PIM interfaces.
disable Disables BFD for all the IPv6 PIM interfaces.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The BFD status for PIM must be enabled before PIM can interact with BFD.

Examples

- -> ipv6 pim bfd-state all-interfaces enable
- -> ipv6 pim bfd-state all-interfaces disable

Release History

Release 8.4.1.R03; command was introduced.

Related Commands

ipv6 pim bfd-state  Enables or disables the registration of PIM with the BFD protocol.
ipv6 pim interface bfd-state Enables or disables BFD monitoring on a specific PIM interface.
show ipv6 pim interface Displays detailed PIM settings for a specific interface.

MIB Objects

alaPimGlobalConfig
alaPimBfdAllInterfaceStatus
ipv6 pim interface bfd-state

Enables or disables BFD monitoring for a specific PIM interface.

`ipv6 pim interface if_name bfd-state {enable | disable}`

**Syntax Definitions**

- `if_name`: The name of an existing IPv6 PIM interface.
- `enable`: Enables BFD for the specified PIM interface.
- `disable`: Disables BFD for the specified PIM interface.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td><code>disable</code></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

|------|------|------|-------|------|-------|------|------|--------------|---------------------------------|------|
| No   | No   | No   | No    | Yes  | Yes   | Yes  | Yes  | Yes          | Yes                            | Yes

**Usage Guidelines**

- Registering PIM with BFD is required at the protocol level before PIM can interact with BFD.
- When BFD is enabled on the specified PIM interface, BFD monitors the connectivity to all neighbors known through the specified interface.

**Examples**

- `-> ipv6 pim interface pimInt1 bfd-state enable`
- `-> ipv6 pim interface pimInt1 bfd-state disable`

**Release History**

Release 8.4.1.R03; command was introduced.
**Related Commands**

- **ipv6 pim bfd-state** Enables or disables the registration of PIM with the BFD protocol.
- **ipv6 pim bfd-state all-interfaces** Enables or disables BFD monitoring for all PIM interfaces in the switch configuration.
- **show ipv6 pim interface** Displays detailed PIM settings for a specific interface.

**MIB Objects**

- **alaPimInterfaceAugTable**
  - **alaPimBfdStatus**
ipv6 pim bidir ssm-compat

Configures the status of the Source-specific Multicast (SSM) compatibility mode. When enabled, an IPv6 BIDIR-PIM router will support receiving MLDv2 SSM joins and process them as a (*,G) join.

ipv6 pim bidir ssm-compat {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th></th>
<th>Administratively enables the IPv6 BIDIR/SSM compatibility mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td>Administratively disables IPv6 BIDIR/SSM compatibility mode.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>6900</th>
<th>X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When the SSM compatibility mode is disabled, MLDv2 SSM joins are ignored by the IPv6 BIDIR-PIM router.
- This command is only applicable if IPv6 BIDIR-PIM is globally enabled for the switch.

Examples

- ipv6 pim bidir ssm-compat enable
- ipv6 pim bidir ssm-compat disable

Release History

Release 8.3.1.R02; command was introduced.
**Related Commands**

*show ipv6 pim sparse* Displays the status of the various global parameters for the IPv6 PIM sparse mode.

**MIB Objects**

alaPimsmGlobalConfig
alaPimsmV6BidirSsmCompat
ipv6 pim bidir fast-join

Configures whether or not an IPv6 BIDIR-PIM router will automatically create (*,G) routes in the hardware as soon as IPv6 BIDIR (*,G) routes are learned.

ipv6 pim bidir fast-join {enable | disable}

Syntax Definitions

| enable | Administratively enables the IPv6 BIDIR-PIM fast join functionality. |
| disable | Administratively disables the IPv6 BIDIR-PIM fast join functionality. |

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is only applicable if IPv6 BIDIR-PIM is globally enabled for the switch.
- When the IPv6 BIDIR fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the IPv6 BIDIR fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

Examples

-> ipv6 pim bidir fast-join enable
-> ipv6 pim bidir fast-join disable

Release History

Release 8.3.1.R02; command was introduced.

Related Commands

| show ipv6 pim sparse | Displays the status of the various global parameters for the IPv6 PIM sparse mode. |

MIB Objects

<table>
<thead>
<tr>
<th>alaPimsmGlobalConfig</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaPimsmV6BidirFastJoin</td>
</tr>
</tbody>
</table>
**ipv6 pim sparse asm-fast-join**

Configures whether or not an IPv6 PIM Sparse router will automatically create (*,G) routes in the hardware as soon as the IPv6 (*,G) routes are learned.

`ipv6 pim sparse asm-fast-join {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Administratively enables the IPv6 PIM Sparse ASM fast join functionality.</td>
</tr>
<tr>
<td>disable</td>
<td>Administratively disables the IPv6 PIM Sparse ASM fast join functionality.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- This command is only supported in the IPv6 PIM Sparse mode.
- When the IPv6 PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (*,G) routes are already created before the actual multicast traffic is received.
- When the IPv6 PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.
- This option should be used with caution due to the complicated nature of IPv6 PIM ASM, which involves forwarding on the shared tree, the sending and receiving of PIM register packets, and switching to the SPT. As a result, only enable the IPv6 ASM fast join function when there are no other locally attached sources, the router is not the RP, and the SPT is disabled.

**Examples**

- `ipv6 pim sparse asm-fast-join enable`
- `ipv6 pim sparse asm-fast-join disable`

**Release History**

Release 8.3.1.R02; command was introduced.
Related Commands

- **show ipv6 pim sparse**
  Displays the status of the various global parameters for the IPv6 PIM sparse mode.

MIB Objects

- `alaPimsmGlobalConfig`
- `alaPimsmV6AsmFastJoin`
**ipv6 pim sparse ssm-fast-join**

Configures whether or not an IPv6 PIM Sparse router will automatically create both IPv6 PIM Sparse and SSM (S,G) routes in the hardware as soon as the IPv6 (S,G) routes are learned.

```
ipv6 pim sparse ssm-fast-join {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Administratively enables the IPv6 PIM SSM fast join functionality.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Administratively disables the IPv6 PIM SSM fast join functionality.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

Not supported in this release.

### Usage Guidelines

- This command is only supported in the IPv6 PIM Sparse mode.
- When the IPv6 PIM Sparse fast join functionality is enabled, convergence of multicast traffic may occur faster because the (S,G) routes are already created before the actual multicast traffic is received.
- When the IPv6 PIM Sparse fast join functionality is disabled (the default), routes are not created in the hardware until the multicast traffic reaches the switch.

### Examples

```
-> ipv6 pim sparse ssm-fast-join enable
-> ipv6 pim sparse ssm-fast-join disable
```

### Release History

Release 8.3.1.R02; command was introduced.

### Related Commands

- `show ipv6 pim sparse` Displays the status of the various global parameters for the IPv6 PIM sparse mode.

### MIB Objects

- `alaPimsmGlobalConfig` `alaPimsmV6SsmFastJoin`
ipv6 pim joinprune-packing

Enable or disable PIM Join/Prune message packing.

ipv6 pim joinprune-packing {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable the PIM Join/Prune message packing.</td>
</tr>
<tr>
<td>disable</td>
<td>Disable the PIM Join/Prune message packing</td>
</tr>
</tbody>
</table>

Defaults

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The value of disable can be used to disable this feature and return to the original operation of PIM where Join/Prune messages are not packed.

Examples

-> ipv6 pim joinprune-packing enable
-> ipv6 pim joinprune-packing disable

Release History

Release 8.6R1; command introduced.
**Related Commands**

show ipv6 pim sparse

Displays the status of the various global parameters for the IPv6 PIM sparse mode.

**MIB Objects**

alaPimGlobalConfig

alaPimV6JoinPruneMsgPackingStatus
**show ipv6 pim sparse**

Displays the status of the various global parameters for the IPv6 PIM sparse mode.

```
-> show ipv6 pim sparse
```

---

**Syntax Definitions**

N/A

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

```
-> show ipv6 pim sparse
Status = disabled,
Keepalive Period = 210,
Max RPs = 32,
Probe Time = 5,
Register Suppress Timeout = 60,
RP Switchover = enabled,
SPT Status = enabled,
BIDIR Status = disabled,
BIDIR Periodic Interval = 60,
BIDIR DF Abort Status = disabled,
BFD Status = disabled,
ASM Fast Join = disabled,
SSM Fast Join = disabled,
BIDIR Fast Join = disabled,
BIDIR SSM Compatibility = disabled,
Register Rate Limit = 100,
Join/Prune Message Packing = enabled,
Register Message packing = force-enabled,
Register MTU = 1500,
Register Triggered Delay = 200
```
output definitions

<table>
<thead>
<tr>
<th>Status</th>
<th>The current global (i.e., switch-wide) status of the IPv6 PIM sparse mode. Options include enabled and disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keepalive Period</td>
<td>The duration of the Keepalive timer. The default value is 210.</td>
</tr>
<tr>
<td>Max RPs</td>
<td>The maximum number of Rendezvous Points (RPs) allowed in the IPv6 PIM-SM domain (1–100). The default value is 32.</td>
</tr>
<tr>
<td>Probe Time</td>
<td>The amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the RP. This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP. Values may range from 1 to 300. The default value is 5.</td>
</tr>
<tr>
<td>Register Suppress Timeout</td>
<td>The amount of time, in seconds, the DR will stop sending registers to the RP once a Register-Stop is received (1–300). The default value is 60.</td>
</tr>
<tr>
<td>RP switchover</td>
<td>The current status of the RP Switchover capability. RP switchover enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated data packet. Options include enabled and disabled. The default setting is enabled.</td>
</tr>
<tr>
<td>SPT Status</td>
<td>The current status of last hop DR switching to the SPT. Options include enabled and disabled. The default setting is enabled.</td>
</tr>
<tr>
<td>BIDIR Status</td>
<td>The current global status of Bidirectional PIM (BIDIR-PIM) for the switch. Options include enabled and disabled (the default).</td>
</tr>
<tr>
<td>BIDIR Periodic Interval</td>
<td>The amount of time, in seconds, between Winner messages the DF sends out to announce its status. The valid range is 0–2000. The default is 60 seconds.</td>
</tr>
<tr>
<td>BIDIR DF Abort Status</td>
<td>Indicates whether or not the Designated Forwarder (DF) election process is aborted when a PIM Hello message is received from a non-Bidirectional PIM (BIDIR-PIM) capable router. Options include enabled and disabled (the default).</td>
</tr>
<tr>
<td>BFD Status</td>
<td>Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is enabled or disabled (the default) for the PIM router.</td>
</tr>
<tr>
<td>ASM Fast Join</td>
<td>The status of the PIM Sparse fast join operation for ASM routes. When enabled, PIM ASM (<em>,G) routes are automatically created in hardware when the routes are initially learned; when disabled (the default), the (</em>,G) routes are not created in hardware until multicast traffic reaches the switch.</td>
</tr>
<tr>
<td>SSM Fast Join</td>
<td>The status of the PIM Sparse fast join operation for PIM Sparse and SSM routes. When enabled, PIM Sparse and SSM (S,G) routes are automatically created in hardware when the routes are initially learned; when disabled (the default), the (S,G) routes are not created in hardware until multicast traffic reaches the switch.</td>
</tr>
<tr>
<td>BIDIR Fast Join</td>
<td>The status of the BIDIR-PIM fast join operation. When enabled, BIDIR-PIM (<em>,G) routes are automatically created in hardware when the routes are initially learned; when disabled (the default), the (</em>,G) routes are not created in hardware until multicast traffic reaches the switch.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BIDIR SSM Compatibility</strong></td>
<td>The status of the SSM compatibility mode. When enabled, a BIDIR-PIM router will accept and process SSM joins as (*,G) joins; when disabled (the default), SSM joins are ignored.</td>
</tr>
<tr>
<td><strong>Register Rate Limit</strong></td>
<td>The per (S,G) register rate limit in packets per second.</td>
</tr>
<tr>
<td><strong>Join/Prune Message Packing</strong></td>
<td>The current status of PIM Join/Prune message packing. Options include enabled and disabled.</td>
</tr>
<tr>
<td><strong>Register Message packing</strong></td>
<td>The current status of PIM Register message packing. Options include enabled, force-enabled and disabled.</td>
</tr>
<tr>
<td><strong>Register MTU</strong></td>
<td>The size of the message in bytes used for PIM packed register messages.</td>
</tr>
<tr>
<td><strong>Register Triggered Delay</strong></td>
<td>The Triggered Register Delay interval in milliseconds.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.4; BIDIR fields added.
Release 8.3.1.R02; **ASM Fast Join, SSM Fast Join, BIDIR Fast Join, and BIDIR SSM Compatibility** fields added.
Release 8.4.1.R02; **Register Rate Limit** field added.
Release 8.6R1; **Join/Prune Message Packing** field added.
Release 8.7R2; **Register Message Packing, Register MTU, Register Trigger Delay** fields added.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 pim sparse admin-state</td>
<td>Enables or disables the IPv6 PIM-SM (sparse mode) globally for IPv6.</td>
</tr>
<tr>
<td>ip pim keepalive-period</td>
<td>Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.</td>
</tr>
<tr>
<td>ip pim max-rps</td>
<td>Configures the maximum number of C-RP routers allowed in the PIM-SM domain.</td>
</tr>
<tr>
<td>ip pim probe-time</td>
<td>Configures the amount of time before the Register Suppression timer expires, at which point the Designated Router (DR) sends a Null Register message to the Rendezvous Point (RP). This allows the RP to refresh the Register-Stop. If the Register Suppression timer expires, the DR will resume encapsulating packets from the source to the RP.</td>
</tr>
<tr>
<td>ip pim register-suppress-timeout</td>
<td>Specifies the period during which a Designated Router (DR) stops sending Register-encapsulated packets to the Rendezvous Point (RP) after receiving a Register-Stop message.</td>
</tr>
<tr>
<td>ipv6 pim rp-switchover</td>
<td>Enables or disables an RP to attempt switching to native forwarding upon receiving the first register-encapsulated packet in the IPv6 PIM domain.</td>
</tr>
<tr>
<td>ipv6 pim register-rate-limit</td>
<td>Specifies the maximum number of PIM Register Packets that the Designated Router (DR) will send per second for each (S,G) entry.</td>
</tr>
<tr>
<td>ipv6 pim spt admin-state</td>
<td>Enables or disables last hop DR switching to the Shortest Path Tree (SPT). If enabled, last hop DR switching to the SPT begins once the first multicast data packet is received.</td>
</tr>
</tbody>
</table>
### PIM Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 pim bidir admin-state</code></td>
<td>Globally enables or disables BIDIR-PIM protocol on the switch.</td>
</tr>
<tr>
<td><code>ip pim df-periodic-interval</code></td>
<td>Configures the time interval at which the DF for each RP address periodically announces its status in a Winner message.</td>
</tr>
<tr>
<td><code>ip pim df-abort</code></td>
<td>Configures whether or not the DF election process is stopped when a PIM Hello message received from a PIM neighbor does not contain the Bidirectional Capable option.</td>
</tr>
<tr>
<td><code>ipv6 pim interface</code></td>
<td>Enables IPv6 PIM and configures statistics on the interface.</td>
</tr>
<tr>
<td><code>ipv6 pim bfd-state</code></td>
<td>Enables or disables BFD for the PIM router.</td>
</tr>
<tr>
<td><code>ipv6 pim sparse asm-fast-join</code></td>
<td>Configures the status of the PIM Sparse fast join operation for ASM routes.</td>
</tr>
<tr>
<td><code>ipv6 pim sparse ssm-fast-join</code></td>
<td>Configures the status of the PIM Sparse fast join operation for both PIM Sparse and SSM routes.</td>
</tr>
<tr>
<td><code>ipv6 pim bidir fast-join</code></td>
<td>Configures the status of the BIDIR-PIM fast join operation.</td>
</tr>
<tr>
<td><code>ipv6 pim bidir ssm-compat</code></td>
<td>Configures the SSM compatibility mode for a BIDIR-PIM router.</td>
</tr>
<tr>
<td><code>ipv6 pim joinprune-packing</code></td>
<td>Enable or disable PIM Join/Prune message packing.</td>
</tr>
<tr>
<td><code>ipv6 pim register-packing</code></td>
<td>Enables or disables the PIM Register Message Packing.</td>
</tr>
<tr>
<td><code>ipv6 pim register-mtu</code></td>
<td>Configures the maximum size of messages used for PIM packed register messages.</td>
</tr>
<tr>
<td><code>ipv6 pim register-delay</code></td>
<td>Configures the Triggered Register Delay interval in milliseconds.</td>
</tr>
</tbody>
</table>

### MIB Objects

- **ALCATEL-IND1-PIM-MIB.mib**
  - `alaPimsmGlobalConfig`
  - `alaPimsmV6AdminStatus`
  - `alaPimsmMaxRPS`
  - `alaPimsmProbeTime`
  - `alaPimsmV6RPSwitchover`
  - `alaPimsmV6AdminSPTConfig`
  - `alaPimsmBidirStatus`
  - `alaPimsmBidirPeriodicInterval`
  - `alaPimsmBidirDFAbort`
  - `alaPimsmV6AsmFastJoin`
  - `alaPimsmV6SsmFastJoin`
  - `alaPimsmV6BidirFastJoin`
  - `alaPimsmV6BidirSsmCompat`
  - `alaPimsmV6RegisterMsgPackingStatus`
  - `alaPimsmV6RegisterMsgPackingStatus`
  - `alaPimsmV6PackedRegisterMsgDelay`

- **alaPimGlobalConfig**
  - `alaPimV6BfdStatus`
  - `alaPimV6JoinPruneMsgPackingStatus`

- **PIM-STD-MIB.mib**
  - `pim`
  - `pimKeepalivePeriod`
  - `pimRegisterSuppressionTime`
show ipv6 pim dense

Displays the status of the various global parameters for the IPv6 PIM dense mode.

show ipv6 pim dense

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 pim dense
Status = enabled,
Source Lifetime = 210,
State Refresh Interval = 60,
State Refresh Limit Interval = 0,
State Refresh TTL = 16
BFD Status = enabled

output definitions

<table>
<thead>
<tr>
<th>Status</th>
<th>The current global (i.e., switch-wide) status of the IPv6 PIM dense mode. Options include enabled and disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Lifetime</td>
<td>The duration of the Keepalive or Source Lifetime timer. The default value is 210.</td>
</tr>
<tr>
<td>State Refresh Interval</td>
<td>The time-interval, in seconds, between successive State Refresh messages originated by the router. The default value is 60.</td>
</tr>
<tr>
<td>State Refresh Limit Interval</td>
<td>Displays the limit at which a router will not forward the State Refresh messages, if they are received at less than the interval. The default value is 0.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>State Refresh TTL</th>
<th>Displays the TTL to be used in the router’s originated State Refresh messages. The default value is 16.</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFD Status</td>
<td>Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is enabled or disabled (the default) for PIM router.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

- **ipv6 pim dense admin-state** Enables or disables IPv6 PIM-DM (dense mode) globally on the switch.
- **ip pim keepalive-period** Configures the period during which the (S,G) Join state will be maintained in the absence of (S,G) Join messages or explicit (S,G) local membership.
- **ip pim state-refresh-interval** Sets the interval between successive State Refresh messages originated by a router.
- **ip pim state-refresh-limit** Sets the limit at which a router will not forward successive State Refresh messages if they are received at less than the interval.
- **ip pim state-refresh-ttl** Sets the Time to Live to be used in a router’s originated State Refresh messages if the data packet’s Time to Live is not recorded.
- **ipv6 pim bfd-state** Enables or disables BFD for the PIM router.

MIB Objects

- ALCATEL-IND1-PIM-MIB.mib
  - alaPimdmGlobalConfig
    - alaPimdmV6AdminStatus
    - alaPimRefreshInterval
    - alaPimdmStateRefreshLimitInterval
    - alaPimdmStateRefreshTimeToLive
  - alaPimGlobalConfig
    - alaPimV6BfdStatus
- PIM-STD-MIB.mib
  - pim
    - pimKeepalivePeriod
**show ipv6 pim ssm group**

Displays the static configuration of IPv6 multicast group mappings for PIM-Source Specific Multicast (SSM).

```
show ipv6 pim ssm group
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

**Examples**

```
-> show ipv6 pim ssm group
```

<table>
<thead>
<tr>
<th>Group Address/Prefix</th>
<th>RP Address</th>
<th>Mode</th>
<th>Override</th>
<th>Precedence</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff00::/8</td>
<td>::</td>
<td>ssm</td>
<td>false</td>
<td>none</td>
<td>enabled</td>
</tr>
<tr>
<td>ff34::/32</td>
<td>::</td>
<td>ssm</td>
<td>false</td>
<td>none</td>
<td>enabled</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Group Address/Prefix</th>
<th>The IPv6 multicast group address along with the prefix length.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>The IPv6 address of the Rendezvous Point (RP) for groups within this group prefix.</td>
</tr>
<tr>
<td>Mode</td>
<td>The IPv6 PIM mode that is used for the groups in this prefix.</td>
</tr>
<tr>
<td>Override</td>
<td>Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).</td>
</tr>
<tr>
<td>Precedence</td>
<td>The precedence value that can be used for this static RP configuration.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays whether this entry is currently enabled or disabled. Options include enabled and disabled.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ipv6 pim ssm group`  
  Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

**MIB Objects**

- `pimStaticRPTable`
  - `pimStaticRPGrpAddress`
  - `pimStaticRPGrpPrefixLength`
  - `pimStaticRPRPAddress`
  - `pimStaticRPImMode`
  - `pimStaticRPOverrideDynamic`
  - `pimStaticRPPrecedence`
  - `pimStaticRPRowStatus`
**show ipv6 pim dense group**

Displays the static configuration of IPv6 multicast group mappings for PIM Dense Mode (DM).

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Group Address/Prefix</th>
<th>RP Address</th>
<th>Mode</th>
<th>Override</th>
<th>Precedence</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff00::/8</td>
<td>::</td>
<td>dm</td>
<td>false</td>
<td>none</td>
<td>enabled</td>
</tr>
<tr>
<td>ff34::/32</td>
<td>::</td>
<td>dm</td>
<td>false</td>
<td>none</td>
<td>enabled</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

**Examples**

```
-> show ipv6 pim dense group
```

```
Group Address/Prefix | RP Address | Mode | Override | Precedence | Status
---------------------|------------|------|----------|------------|--------
ff00::/8             | ::         | dm   | false    | none       | enabled |
ff34::/32            | ::         | dm   | false    | none       | enabled |
```

**output definitions**

- **Group Address/Pref**: The IPv6 multicast group address along with the prefix length.
- **RP Address**: The IPv6 address of the Rendezvous Point (RP) for groups within this group prefix.
- **Mode**: The IPv6 PIM mode that is used for the groups in this prefix.
- **Override**: Specifies this static RP configuration to override the dynamically learned RP information for the specified group(s).
- **Precedence**: The precedence value that can be used for this static RP configuration.
- **Status**: Displays whether this entry is currently enabled or disabled. Options include **enabled** and **disabled**.
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**ipv6 pim dense group**

Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

**MIB Objects**

alaPimdmDenseGroupTable
- alaPimdmDenseGroupGrpAddress
- alaPimdmDenseGroupGrpPrefixLength
- alaPimdmDenseGroupOverrideDynamic
- alaPimdmDenseGroupPrecedence
- alaPimdmDenseGroupRowStatus
**show ipv6 pim interface**

Displays detailed IPv6 PIM settings for a specific interface. In general, it displays IPv6 PIM settings for all the interfaces if no argument is specified.

**show ipv6 pim interface [if_name]**

---

**Syntax Definitions**

*if_name*  
The name of the interface.

---

**Defaults**

By default, a summary list of all IPv6 PIM interfaces is displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

To view more detailed information about a particular interface, specify the interface name in the command line. Additional information includes Triggered Hello Interval, Hello Holdtime, Prune Delay status and value, Override Interval, LAN Delay status, Generation ID status, and Join/Prune Holdtime.

---

**Examples**

-> show ipv6 pim interface

Total 0 Interfaces

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Designated Router</th>
<th>Hello Interval</th>
<th>J/P Interval Status</th>
<th>Oper Status</th>
<th>BFD Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-5</td>
<td>fe80::2d0:95ff:feac:a537</td>
<td>30</td>
<td>60</td>
<td>enabled</td>
<td>disabled</td>
</tr>
<tr>
<td>vlan-30</td>
<td>fe80::2d0:95ff:feac:a537</td>
<td>30</td>
<td>60</td>
<td>disabled</td>
<td>disabled</td>
</tr>
<tr>
<td>vlan-40</td>
<td>fe80::2d0:95ff:fee2:6ee3</td>
<td>30</td>
<td>60</td>
<td>enabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

-> show ipv6 pim interface vlan-5

Interface Name = vlan-5,
IP Address     = fe80::2d0:95ff:fee2:6ee3,
Designated Router = fe80::2d0:95ff:fee2:a537,
Hello Interval  = 30,
Triggered Hello Interval = 5,
Hello HoldTime   = 105,
Join/Prune Interval = 60,
Join/Prune HoldTime = 210,
Propagation (Prune) Delay = 500,
Override Interval = 2500,
Generation ID = 0x4717be4d,
DR Priority = 1,
DR Priority Enabled = true,
Lan Delay Enabled = true,
Effective Propagation Delay = 500,
Effective Override Interval = 2500,
Suppression Enabled = true,
Stub Interface = false,
Prune Limit Interval = 60,
Graft Retry Interval = 3,
State Refresh Enabled = true,
BiDir Capable = false,
DF Election Robustness = 3,
Operational Status = enabled,
BFD Status = disabled,
Join/Prune MTU = 1000,
Join/Prune Triggered Delay = 100

output definitions

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>The name of the IPv6 PIM interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 address</td>
<td>Specifies the IPv6 address of the specified interface.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>The primary IP address for the Designated Router (DR). The DR acts on behalf of any directly-connected hosts with respect to the PIM-SM protocol. Only one router in the LAN will act as the DR.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The frequency at which PIM Hello messages are transmitted on a specified interface. Values may range from 1 to 18000. The default value is 30.</td>
</tr>
<tr>
<td>Join/Prune Interval</td>
<td>The Join/Prune interval for the associated interface. The Join/Prune interval is the interval at which periodic PIM-SM Join/Prune messages are sent. Values may range from 0 to 18000. The default value is 60.</td>
</tr>
<tr>
<td>Triggered Hello Interval</td>
<td>The current Triggered Hello Interval. This value indicates the maximum time, in seconds, before a triggered PIM Hello message is transmitted on the corresponding interface. Values may range from 0 to 60. The default value is 5.</td>
</tr>
<tr>
<td>Hello Holdtime</td>
<td>The current Hello Holdtime value. This value indicates the maximum amount of time, in seconds, Hello messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 105.</td>
</tr>
<tr>
<td>Join/Prune Holdtime</td>
<td>The current Join/Prune Holdtime value. This value indicates the maximum amount of time, in seconds, Join/Prune messages will be held before they are considered invalid. Values may range from 0 to 65535. The default value is 210.</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>The expected propagation delay between PIM routers on the network. Values may range from 0 to 32767. The default value is 500.</td>
</tr>
<tr>
<td>Override Interval</td>
<td>The current Override Interval. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by a router is dictated by this number. Values may range from 0 to 65535. The default value is 2500.</td>
</tr>
</tbody>
</table>
### PIM Commands: show ipv6 pim interface

<table>
<thead>
<tr>
<th>Output Definitions (continued)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Generation ID Option</strong></td>
<td>The value of the Generation ID this router inserted in the last PIM Hello message it sent on this interface.</td>
</tr>
<tr>
<td><strong>DR Priority</strong></td>
<td>Displays the Designated Router priority for each interface. This value is used in determining the Designated Router on an interface. Values may range from 1 to 192. A higher numeric value denotes a higher priority. Note that priority-based election is used only if all routers on the interface are using the DR priority option. The default value is 1.</td>
</tr>
<tr>
<td><strong>Lan Delay Enabled</strong></td>
<td>Options include <strong>true</strong> and <strong>false</strong>. The value will be true if all neighbors on the interface are using the LAN Prune Delay option. Otherwise, the setting will be false.</td>
</tr>
<tr>
<td><strong>Effective Propagation Delay</strong></td>
<td>The Effective Propagation Delay on this interface.</td>
</tr>
<tr>
<td><strong>Effective Override Interval</strong></td>
<td>The Effective Override Interval on this interface.</td>
</tr>
<tr>
<td><strong>Suppression Enabled</strong></td>
<td>Specifies whether the Join suppression is enabled on this interface.</td>
</tr>
<tr>
<td><strong>DR Priority Enabled</strong></td>
<td>Evaluates to <strong>true</strong> if all routers on this interface are using the DR Priority option.</td>
</tr>
<tr>
<td><strong>Stub Interface</strong></td>
<td>Specifies whether this interface is a 'stub interface'. If this is <strong>true</strong>, then no PIM packets are sent out on this interface, and any received PIM packets are ignored.</td>
</tr>
<tr>
<td><strong>Prune Limit Interval</strong></td>
<td>The minimum interval that must transpire between two successive Prunes sent by a router. This is used only with PIM-DM. Values may range from 0 to 65535. The default value is 60.</td>
</tr>
<tr>
<td><strong>Graft Retry Interval</strong></td>
<td>Displays the time-interval a router waits for a Graft acknowledgment before resending a Graft on the interface. This is only used with PIM-DM. Values may range from 0 to 65535. The default value is 3.</td>
</tr>
<tr>
<td><strong>SR Priority Enabled</strong></td>
<td>Evaluates to <strong>true</strong> if all routers on this interface are using the State Refresh option. This is used only by PIM-DM.</td>
</tr>
<tr>
<td><strong>BiDir Capable</strong></td>
<td>Evaluates to <strong>true</strong> if all routers on this interface are using the Bidirectional Capable option. This is used only by BIDIR-PIM.</td>
</tr>
<tr>
<td><strong>DF Election Robustness</strong></td>
<td>The minimum number of PIM Designated Forwarder (DF) Election messages that must be lost to determine that the DF Election process has failed for this interface. This is used only by BIDIR-PIM.</td>
</tr>
<tr>
<td><strong>Operational Status</strong></td>
<td>The current operational status of the corresponding interface. Options include <strong>enabled</strong> and <strong>disabled</strong>. This value indicates whether the IPv6 interface is operationally up. For example, if PIM is enabled on the interface, but the interface is currently down, this field will display as disabled. The default setting is <strong>disabled</strong>. To enable or disable PIM on an interface, refer to the <strong>ipv6 pim interface</strong> command on page 34-163. To globally enable or disable PIM on the switch, refer to the <strong>ipv6 pim sparse admin-state</strong> command on page 34-133 and <strong>ipv6 pim dense admin-state</strong> command on page 34-137.</td>
</tr>
<tr>
<td><strong>BFD Status</strong></td>
<td>Indicates whether the Bidirectional Forwarding Detection (BFD) protocol is <strong>enabled</strong> or <strong>disabled</strong> (the default) for the PIM interface. Configured through the <strong>ipv6 pim interface bfd-state</strong> command.</td>
</tr>
<tr>
<td><strong>Join/Prune MTU</strong></td>
<td>The configured PIM Join/Prune packet MTU for this interface.</td>
</tr>
<tr>
<td><strong>Join/Prune Triggered Delay</strong></td>
<td>The triggered Join/Prune delay.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; **BiDir Capable** and **DF Election Robustness** fields added.
Release 8.6R1; **Join/Prune MTU** and **Join/Prune Triggered** Delay fields added.

**Related Commands**

**ipv6 pim interface**

Enables IPv6 PIM and configures statistics on the interface.

**MIB Objects**

```
pimInterfaceTable
   pimInterfaceIfIndex
   pimInterfaceIPVersion
   pimInterfaceAddressType
   pimInterfaceAddress
   pimInterfaceGenerationIDValue
   pimInterfaceDR
   pimInterfaceDRPriority
   pimInterfaceDRPriorityEnabled
   pimInterfaceHelloInterval
   pimInterfaceTrigHelloInterval
   pimInterfaceHelloHoldtime
   pimInterfaceJoinPruneInterval
   pimInterfaceJoinPruneHoldtime
   pimInterfaceDFElectionRobustness
   pimInterfaceLanDelayEnabled
   pimInterfacePropagationDelay
   pimInterfaceOverrideInterval
   pimInterfaceEffectPropagDelay
   pimInterfaceEffectOverrideIvl
   pimInterfaceSuppressionEnabled
   pimInterfaceBidirCapable
   pimInterfaceDomainBorder
   pimInterfaceStubInterface
   pimInterfacePruneLimitInterval
   pimInterfaceGraftRetryInterval
   pimInterfaceSRPriorityEnabled
   pimInterfaceStatus
```

```
alaPimInterfaceAugTable
   alaPimInterfaceBfdStatus
   alaPimInterfaceJoinPruneMtu
   alaPimInterfaceJoinPruneDelay
```
show ipv6 pim neighbor

Displays a list of active IPv6 PIM neighbors.

**show ipv6 pim neighbor [ipv6_address] [if_name]**

**Syntax Definitions**

- **ipv6_address**: The IPv6 address for the PIM neighbor.
- **if_name**: The name of the interface.

**Defaults**

If the neighbor’s IPv6 address or interface name is not specified, the entire IPv6 PIM neighbor table is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view more detailed information about a particular neighbor, specify the neighbor's IPv6 address or the associated interface name in the command line. Additional information will be displayed, which includes LAN Prune Delay, Override Interval, TBit field, State Refresh capable, and Designated Router option status.

**Examples**

```
-> show ipv6 pim neighbor
Neighbor Address Interface Name Uptime Expires DR Pri
-----------------------------------------------+-------------------+----------+---------+-----
fe80::2d0:95ff:feac:a537 vlan-30 02h:56m:51s 00h:01m:28s 1
```

If a specific neighbor address is specified in the command line, detailed information for the corresponding neighbor only displays:

```
-> show ipv6 pim neighbor fe80::2d0:95ff:feac:a537
  vlan-30
  Neighbor IPv6 Address = fe80::2d0:95ff:feac:a537,
  Uptime = 02h:57m:09s,
  Expires = 00h:01m:40s,
  Lan Prune Delay Present = True,
  Propagation Delay = 500,
  Override Interval = 2500,
  TBit Field = True,
  Gen ID Present = True,
```
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gen ID Value</td>
<td>0x7720c123</td>
</tr>
<tr>
<td>BiDir Capable</td>
<td>False</td>
</tr>
<tr>
<td>DR Priority Present</td>
<td>True</td>
</tr>
<tr>
<td>DR Priority</td>
<td>1</td>
</tr>
<tr>
<td>State Refresh Capable</td>
<td>True</td>
</tr>
<tr>
<td>Secondary Addresses:</td>
<td>3000::11</td>
</tr>
<tr>
<td>Neighbor IPv6 Address</td>
<td>fe80::2d0:95ff:feac:a537</td>
</tr>
<tr>
<td>Uptime</td>
<td>03h:57m:03s</td>
</tr>
<tr>
<td>Expires</td>
<td>00h:01m:20s</td>
</tr>
<tr>
<td>Lan Prune Delay Present</td>
<td>True</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>500</td>
</tr>
<tr>
<td>Override Interval</td>
<td>2500</td>
</tr>
<tr>
<td>TBit Field</td>
<td>True</td>
</tr>
<tr>
<td>Gen ID Present</td>
<td>True</td>
</tr>
<tr>
<td>Gen ID Value</td>
<td>0x7720c123</td>
</tr>
<tr>
<td>BiDir Capable</td>
<td>False</td>
</tr>
<tr>
<td>DR Priority Present</td>
<td>True</td>
</tr>
<tr>
<td>DR Priority</td>
<td>1</td>
</tr>
<tr>
<td>State Refresh Capable</td>
<td>True</td>
</tr>
<tr>
<td>Secondary Addresses:</td>
<td>4000::11</td>
</tr>
</tbody>
</table>

If a specific interface name is specified in the command line, detailed information corresponding to all neighbors on the specified interface only displays:

-> show IPv6 pim neighbor vlan-30

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor IPv6 Address</td>
<td>fe80::2d0:95ff:feac:a537</td>
</tr>
<tr>
<td>Uptime</td>
<td>02h:57m:09s</td>
</tr>
<tr>
<td>Expires</td>
<td>00h:01m:40s</td>
</tr>
<tr>
<td>Lan Prune Delay Present</td>
<td>True</td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>500</td>
</tr>
<tr>
<td>Override Interval</td>
<td>2500</td>
</tr>
<tr>
<td>TBit Field</td>
<td>True</td>
</tr>
<tr>
<td>Gen ID Present</td>
<td>True</td>
</tr>
<tr>
<td>Gen ID Value</td>
<td>0x7720c123</td>
</tr>
<tr>
<td>BiDir Capable</td>
<td>False</td>
</tr>
<tr>
<td>DR Priority Present</td>
<td>True</td>
</tr>
<tr>
<td>DR Priority</td>
<td>1</td>
</tr>
<tr>
<td>State Refresh Capable</td>
<td>True</td>
</tr>
<tr>
<td>Secondary Addresses:</td>
<td>3000::11</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor IPv6 Address</td>
<td>The IPv6 address of the active PIM neighbor.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The name of the IPv6 PIM interface that is used to reach the neighbor.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time since this PIM neighbor last became a neighbor of the local router, displayed in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Expires</td>
<td>The minimum amount of time remaining before the PIM neighbor will be aged out, displayed in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>LAN Prune Delay present</td>
<td>Specifies whether this neighbor is using the LAN Prune Delay option. Options include <strong>true</strong> or <strong>false</strong>.</td>
</tr>
</tbody>
</table>
PIM Commands

show ipv6 pim neighbor

**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagation Delay</td>
<td>The value of the propagation-delay field of the LAN prune-delay option received from this neighbor. A value of 0 indicates that no LAN prune-delay option was received from this neighbor.</td>
</tr>
<tr>
<td>Override Interval</td>
<td>The current Override Interval of the LAN prune-delay option received from this neighbor. This value is used to avoid synchronization of override messages when multiple downstream routers share a multi-access link. The sending of override messages is delayed at random time intervals. The amount of randomization used by the neighboring router is dictated by this number. Values may range from 0 to 65535. A value of 0 indicates that no LAN prune-delay option was received from this neighbor.</td>
</tr>
<tr>
<td>TBit field</td>
<td>The value of the Tbit field of the LAN prune-delay option received from this neighbor. The Tbit specifies the ability of the neighbor to disable Join suppression.</td>
</tr>
<tr>
<td>Gen ID present</td>
<td>Specifies whether this neighbor is using Generation ID option. Options include <code>true</code> or <code>false</code>.</td>
</tr>
<tr>
<td>Gen ID Value</td>
<td>The value of the Generation ID in the last PIM Hello message received from this neighbor.</td>
</tr>
<tr>
<td>BiDir Capable</td>
<td>Specifies whether this neighbor is using the Bidirectional-PIM Capable option.</td>
</tr>
<tr>
<td>DR Priority Present</td>
<td>Displays whether the neighbor is using the Designated Router option. Options include <code>true</code> or <code>false</code>.</td>
</tr>
<tr>
<td>DR priority</td>
<td>The value of the Designated Router Priority in the last PIM Hello message received from this neighbor.</td>
</tr>
<tr>
<td>State Refresh Capable</td>
<td>Displays whether the neighbor is capable of receiving State Refresh messages. Options include <code>true</code> or <code>false</code>.</td>
</tr>
<tr>
<td>Secondary Addresses</td>
<td>The secondary IPv6 address of this PIM neighbor.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

N/A
**MIB Objects**

pimNeighborTable
- pimNeighborIfIndex
- pimNeighborAddressType
- pimNeighborAddress
- pimNeighborGenerationIDPresent
- pimNeighborGenerationIDValue
- pimNeighborUpTime
- pimNeighborExpiryTime
- pimNeighborDRPriorityPresent
- pimNeighborDRPriority
- pimNeighborLanPruneDelayPresent
- pimNeighborTBit
- pimNeighborPropagationDelay
- pimNeighborOverrideInterval
- pimNeighborBidirCapable
- pimNeighborSRCapable

pimNbrSecAddressTable
- pimNbrSecAddressIfIndex
- pimNbrSecAddressType
- pimNbrSecAddressPrimary
- pimNbrSecAddress
show ipv6 pim static-rp

Displays the IPv6 PIM Static RP table, which includes IPv6 multicast group address/prefix length, the static Rendezvous Point (RP) address, and the current status of the static RP configuration (i.e., enabled or disabled).

show ipv6 pim static-rp

---

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the group prefixes configured for two or more rows in this table overlap, the row with the greatest prefix length value is used for the overlapping range.

Examples

`-> show ipv6 pim static-rp`

<table>
<thead>
<tr>
<th>Group Address/Pref Length</th>
<th>RP Address</th>
<th>Mode</th>
<th>Override</th>
<th>Precedence</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff00::/8</td>
<td>3000::11</td>
<td>asm</td>
<td>false</td>
<td>none</td>
<td>enabled</td>
</tr>
<tr>
<td>ff08::/32</td>
<td>2100::8</td>
<td>bidir</td>
<td>false</td>
<td>none</td>
<td>enabled</td>
</tr>
</tbody>
</table>

output definitions

- **Group Address/Pref Length**: The IPv6 multicast group address along with the prefix length.
- **RP Address**: The IPv6 address of the RP that is mapped for the groups within the group prefix. This field is set to zero, if the specified IPv6 PIM mode is SSM or DM.
- **Mode**: The PIM mode to be used for groups in this prefix. The possible values include `asm`, `ssm`, `dm`, or `bidir`.
- **Override**: Specifies that this static RP configuration can override the dynamically learned RP information for the specified group(s).
**output definitions**

| Precedence | The precedence value that is used for this static RP configuration. |
| Status | Displays whether the static RP configuration is currently enabled or disabled. Options include enabled and disabled. |

### Release History

Release 7.1.1; command was introduced.
Release 7.3.4; bidir mode support added.

### Related Commands

**ipv6 pim static-rp**

Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

### MIB Objects

pimStaticRPTable
  - pimStaticRPAddressType
  - pimStaticRPGrpAddress
  - pimStaticRPGrpPrefixLength
  - pimStaticRPRPAddress
  - pimStaticRPPimMode
  - pimStaticRPOverrideDynamic
  - pimStaticRPPrecedence
  - pimStaticRPRowStatus
  - pimStaticRPStorageType
show ipv6 pim anycast-rp

Displays the anycast RP table, which includes the anycast RP address, the RP address, if its the local router, and the current status of the anycast RP configuration.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

```
-> show ipv6 pim anycast-rp
Anycast RP Address      Router Address      Local    Status
---------------------+-------------------+---------+---------
2001::1           3001::1           true     enabled
2001::1           3001::2           false    enabled
```

output definitions

<table>
<thead>
<tr>
<th>Anycast RP Address</th>
<th>The anycast RP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Address</td>
<td>The router IPv6 address that is a member of the anycast RP set.</td>
</tr>
<tr>
<td>Local</td>
<td>Displays whether this entry corresponds to the local router. The value will display true if this entry corresponds to the local router and false if it does not correspond to the local router.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays whether the anycast RP configuration is currently enabled or disabled. To change the current status, refer to the ipv6 pim anycast-rp command.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.6R2; command introduced.

**Related Commands**

- `ipv6 pim anycast-rp`  
  Configures the anycast RP set, which is the set of all routers that would act as the RP.

**MIB Objects**

- `pimAnycastRPSetsTable`
  
  - `pimAnycastRPSetsAddressType`
  
  - `pimAnycastRPSetsAnycastAddress`
  
  - `pimAnycastRPSetsRouterAddress`
  
  - `pimAnycastRPSetsLocalRouter`
  
  - `pimAnycastRPSetsRowStatus`
show ipv6 pim group-map

Displays the IPv6 PIM group mapping table.

show ipv6 pim group-map [bsr | static-rp | ssm | dense]

Syntax Definitions

N/A

Defaults

If the keywords **bsr**, **static-rp**, **ssm**, or **dense** are included in the command line, then only the entries that were created by the specified origin are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If static RP configuration is being used, this information is obtained from those static RP addresses that are defined through the **ipv6 pim static-rp** command. As long as the RP addresses defined in the static RP set are reachable, they will be added to the group mapping table.
- If the IPv6 multicast groups are mapped to the mode DM or SSM, then the entries created by local SSM address range configuration using the **ipv6 pim ssm group** command and local Dense Mode address range configuration using the **ipv6 pim dense group** command are displayed.
- If the bootstrap mechanism is being used, this information is obtained from received Candidate-RP advertisements (when the local router is the BSR; when the local router is not the BSR, this information is obtained from received bootstrap messages).

Examples

```bash
-> show ipv6 pim group-map
Origin   Group Address/Pref Length   RP Address    Mode  Precedence
---------+---------------------------+-------------+-----+----------
BSR      ff00::/8                    2000::8       bidir 192
BSR      ff00::/8                    3000::11      asm  192
BSR      ff00::/8                    4000::7       asm  192
SSM      ff33::/32                                 ssm

-> show ipv6 pim group-map bsr
Origin   Group Address/Pref Length   RP Address    Mode  Precedence
---------+---------------------------+-------------+-----+----------
BSR      ff00::/8                    2000::8       bidir 192
```
BSR       ff00::/8                    3000::11      asm   192
BSR       ff00::/8                    4000::7       asm   192

-> show ipv6 pim group-map ssm

<table>
<thead>
<tr>
<th>Origin</th>
<th>Group Address/Pref Length</th>
<th>RP Address</th>
<th>Mode</th>
<th>Precedence</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSM</td>
<td>ff33::/32</td>
<td></td>
<td>ssm</td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

**Origin**
The mechanism by which the PIM mode and RP for the group were learned. The possible values include 'static RP' for local static RP configuration, 'static SSM' for both static SSM group configuration and Dense Mode Group configuration, and 'BSR' for the PIM Bootstrap Router mechanism.

**Group Address/Prefix Length**
The IPv6 multicast group address along with the prefix length.

**RP Address**
The IPv6 address of the Rendezvous Point to be used for groups within the group prefix.

**Mode**
The IPv6 PIM mode to be used for groups in this prefix. The possible values include **asm**, **ssm**, **dm**, or **bidir**.

**Mapping Precedence**
The precedence value of a particular row, that determines which row applies to a given group address. Numerically higher values for this object indicate lower precedences, with the value zero denoting the highest precedence.

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; **bidir** mode support added.

**Related Commands**

**ipv6 pim static-rp**
Adds, modifies, or deletes a static RP for an IPv6 multicast group (“modifies” applies only to the RP address, since the table is indexed from group address and prefix length parameters).

**ipv6 pim ssm group**
Statically maps the specified IPv6 multicast group(s) to the PIM Source Specific Multicast mode (SSM).

**ipv6 pim dense group**
Statically maps the specified IPv6 multicast group(s) to the PIM Dense mode (DM).

**MIB Objects**

pimGroupMappingTable
  pimGroupMappingOrigin
  pimGroupMappingAddressType
  pimGroupMappingGrpAddress
  pimGroupMappingGrpPrefixLength
  pimGroupMappingRPAddressType
  pimGroupMappingRPAddress
  pimGroupMappingPimMode
  pimGroupMappingPrecedence
show ipv6 pim candidate-rp

Displays the IPv6 multicast groups for which the local router advertises itself as a Candidate-RP.

show ipv6 pim candidate-rp

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples
-> show ipv6 pim candidate-rp
RP Address Group Address Priority Interval Mode Status
-------------------------------------------------------------
2000::8 ff00::/8 192 60 bidir enabled

output definitions

<table>
<thead>
<tr>
<th>RP Address</th>
<th>An IPv6 unicast address that is advertised as the Candidate-Rendezvous Point (RP).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The IPv6 multicast group address along with the prefix length. This is the group for which the local router advertises itself as a C-RP.</td>
</tr>
<tr>
<td>Priority</td>
<td>The C-RP router’s priority. The lower the value, the higher the priority.</td>
</tr>
<tr>
<td>Interval</td>
<td>The time interval at which the C-RP advertisements are sent to the BSR.</td>
</tr>
<tr>
<td>Mode</td>
<td>Whether or not the Group Address is for a PIM-SM group or a Bidirectional PIM (BIDIR-PIM) group.</td>
</tr>
<tr>
<td>Status</td>
<td>The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.</td>
</tr>
</tbody>
</table>
**Release History**
Release 7.1.1; command was introduced.
Release 7.3.4; **Mode** field added.

**Related Commands**

**ipv6 pim candidate-rp**
Configures the local router as the Candidate-Rendezvous Point (C-RP) for a specified IPv6 multicast group(s).

**MIB Objects**

`pimBsrCandidateRPTable`
- `pimBsrCandidateRPAddressType`
- `pimBsrCandidateRPAddress`
- `pimBsrCandidateRGroupAddress`
- `pimBsrCandidateRGroupPrefixLength`
- `pimBsrCandidateRPBidir`
- `pimBsrCandidateRPAdvTimer`
- `pimBsrCandidateRPPriority`
- `pimBsrCandidateRPAdvInterval`
- `pimBsrCandidateRPHoldtime`
- `pimBsrCandidateRPPriority`
- `pimBsrCandidateRPStorageType`
show ipv6 pim cbsr

Displays the IPv6 Candidate-BSR information that is used in the Bootstrap messages.

show ipv6 pim cbsr

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> show ipv6 pim cbsr
CBSR Address = 3000::7,
Status = enabled,
CBSR Priority = 0,
Hash Mask Length = 126,
Elected BSR = False,
Timer = 00h:00m:00s

**output definitions**

- **CBSR Address**: An IPv6 unicast address that the local router uses to advertise itself as a Candidate-BSR.
- **Status**: The current status of this entry. The status is shown as enabled only if the IPv6 PIM-SM is globally enabled and the IPv6 PIM interface is enabled.
- **CBSR Priority**: The value for the local router as a Candidate-BSR. The higher the value, the higher the priority.
- **Hash Mask Length**: The hash mask length that is advertised in the bootstrap messages (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for an IPv6 multicast group).
**IPv6 PIM Commands**

`show ipv6 pim cbsr`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ipv6 pim cbsr` Configures the Candidate-BSR information that is used in the Bootstrap messages.

**MIB Objects**

- `pimBSrCandidateBSRTable`
  - `pimBsrCandidateBSRZoneIndex`
  - `pimBsrCandidateBSRAddressType`
  - `pimBsrCandidateBSRAddress`
  - `pimBsrCandidateBSRPriority`
  - `pimBsrCandidateBSRHashMaskLength`
  - `pimBsrCandidateBSRElectedBSR`
  - `pimBsrCandidateBSRBootstrapTimer`
  - `pimBsrCandidateBSRStatus`

**output definitions**

<table>
<thead>
<tr>
<th>Elected BSR</th>
<th>Specifies whether the local router is the elected BSR.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer</td>
<td>The time value that is remaining before the local router originates the next Bootstrap message. This value is zero if this router is not the elected BSR.</td>
</tr>
</tbody>
</table>
show ipv6 pim bsr

Displays information about the elected IPv6 BSR.

show ipv6 pim bsr

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> show ipv6 pim bsr`

BSR Address = 3000::7,
BSR Priority = 192,
Hash Mask Length = 126,
Expiry Time = 00h:01m:35s

**output definitions**

- **BSR Address**: The IPv6 unicast address of the elected BSR.
- **BSR Priority**: The priority value of the elected BSR. The higher the value, the higher the priority.
- **Hash Mask Length**: The hash mask length that is advertised in the Bootstrap messages by the elected BSR (the length of the mask is used in the hash function when computing the Rendezvous Point (RP) for a multicast group.
- **Expiry Time**: The minimum time remaining before the elected BSR will be declared down.

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

**ipv6 pim cbsr**  
Configures the Candidate-BSR information that is used in the Bootstrap messages.

**MIB Objects**

- `pimBsrElectedBSRTable`
  - `pimBsrElectedBSRZoneIndex`
  - `pimBsrElectedBSRAddressType`
  - `pimBsrElectedBSRAddress`
  - `pimBsrElectedBSRPriority`
  - `pimBsrElectedBSRHashMaskLength`
  - `pimBsrElectedBSRExpiryTime`
show ipv6 pim groute

Displays (*,G) routing table entries for IPv6 PIM.

show ipv6 pim groute [group_address]

Syntax Definitions

group_address

The IPv6 address of the Multicast Group.

Defaults

By default, entire (*,G) routing table is displayed. To view more detailed (*,G) state information about a particular group, specify the group address in the command line.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

When the group_address is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.

Examples

-> show ipv6 pim groute
Total 1 (*,G)

<table>
<thead>
<tr>
<th>Group Address</th>
<th>RP Address</th>
<th>RPF Interface</th>
<th>UpTime</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff08::2</td>
<td>2000::8</td>
<td>vlan-200</td>
<td>00h:05m:42s</td>
<td>bidir</td>
</tr>
<tr>
<td>ff0e::7</td>
<td>5ffe::3</td>
<td>vlan-4</td>
<td>00h:01m:23s</td>
<td>asm</td>
</tr>
</tbody>
</table>

-> show ipv6 pim groute ff0e::7
(*,ff0e::7)

    UpTime          = 00h:01m:28s
    RP Address      = 5ffe::3,
    PIM Mode        = ASM,
    PIM Mode Origin = BSR,
    Upstream Join State = Not Joined,
    Upstream Join Timer = 00h:00m:00s,
    Upstream Neighbor = fe80::220:fcff:fele:2455,
    RPF Interface   = vlan-4,
    RPF Next Hop    = fe80::220:fcff:fele:2455,
    RPF Route Protocol = Static,
    RPF Route Address = 5ffe::3/128,
PIM Commands

```
RPF Route Metric Pref  = 10,
RPF Route Metric      = 10,
Interface Specific State:
  vlan-3
    UpTime             = 00h:01m:28s,
    Local Membership   = False,
    Join/Prune State   = Joined,
    Prune Pending Timer= 00h:00m:00s,
    Join Expiry Timer  = 00h:02m:02s,
    Assert State       = Loser,
    Assert Timer       = 00h:01m:32s,
    Assert Winner Address= fe80::220:fcff:fe1e:2454,
    Assert Winner Metric Pref = 9 (rpt),
    Assert Winner Metric = 10,
  vlan-4
    UpTime             = 00h:00m:00s,
    Local Membership   = False,
    Join/Prune State   = No Info,
    Prune Pending Timer= 00h:00m:00s,
    Join Expiry Timer  = 00h:00m:00s,
    Assert State       = No Info,
    Assert Timer       = 00h:00m:00s,
  vlan-5
    UpTime             = 00h:00m:00s,
    Local Membership   = False,
    Join/Prune State   = No Info,
    Prune Pending Timer= 00h:00m:00s,
    Join Expiry Timer  = 00h:00m:00s,
    Assert State       = No Info,
    Assert Timer       = 00h:00m:00s,
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group-address</td>
<td>The IPv6 Multicast Group Address.</td>
</tr>
<tr>
<td>RP Address</td>
<td>The address of the Rendezvous Point (RP) for the group.</td>
</tr>
<tr>
<td>RPF Interface</td>
<td>The RPF interface towards the RP. The ifIndex is converted to the if-name</td>
</tr>
<tr>
<td></td>
<td>for the display.</td>
</tr>
<tr>
<td>UpTime</td>
<td>The time since this entry was created.</td>
</tr>
<tr>
<td>Mode</td>
<td>Whether this entry represents an asm, (Any Source Multicast) or bidir</td>
</tr>
<tr>
<td></td>
<td>(Bidirectional PIM) group.</td>
</tr>
<tr>
<td>Pim Mode Origin</td>
<td>The mechanism by which the PIM mode and RP for the group were learned.</td>
</tr>
<tr>
<td>Upstream Join State</td>
<td>Whether the local router should join the RP tree for the group.</td>
</tr>
<tr>
<td>Upstream Join Timer</td>
<td>The time remaining before the local router next sends a periodic (*,G)</td>
</tr>
<tr>
<td></td>
<td>Join message on the RPF IfIndex.</td>
</tr>
<tr>
<td>Upstream Neighbor</td>
<td>The primary address of the neighbor on the RPF Interface that the local</td>
</tr>
<tr>
<td></td>
<td>router is sending periodic (*,G) join messages to.</td>
</tr>
<tr>
<td>RPF Next Hop</td>
<td>The address of the RPF next hop towards the RP.</td>
</tr>
<tr>
<td>RPF Route Protocol</td>
<td>The routing mechanism through which the route used to find the RPF</td>
</tr>
<tr>
<td></td>
<td>interface towards the RP was learned.</td>
</tr>
<tr>
<td>RPF Route Address/Prefix Length</td>
<td>The IPv6 address combined with the prefix length identifies the route used</td>
</tr>
<tr>
<td></td>
<td>to find the RPF interface towards the RP.</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Metric Pref</td>
<td>The metric preference of the route used to find the RPF interface towards the RP.</td>
</tr>
<tr>
<td>Route Metric</td>
<td>The routing metric of the route used to find the RPF interface towards the RP.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The interface name that corresponds to the ifIndex.</td>
</tr>
<tr>
<td>Local Membership</td>
<td>Whether the local router has (*,G) local membership on this interface.</td>
</tr>
<tr>
<td>Join Prune State</td>
<td>The state resulting from (*,G) Join/Prune messages received on this interface.</td>
</tr>
<tr>
<td>Prune Pending Timer</td>
<td>The time remaining before the local router acts on a (*,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.</td>
</tr>
<tr>
<td>Join Expiry Timer</td>
<td>The time remaining before (*,G) Join state for this interface expires.</td>
</tr>
<tr>
<td>Assert State</td>
<td>The (*,G) Assert state for this interface. The possible values are No Info, Winner or Loser.</td>
</tr>
<tr>
<td>Assert Timer</td>
<td>If Assert State is 'Winner', this is the time remaining before the local router next sends a (<em>,G) Assert message on this interface. If the Assert State is 'Loser', this is the time remaining before the (</em>,G) assert state expires.</td>
</tr>
<tr>
<td>Assert Winner Address</td>
<td>If the Assert State is 'Loser', this is the address of the assert winner.</td>
</tr>
<tr>
<td>Assert Winner Metric Pref</td>
<td>If the Assert State is 'Loser', this is the metric preference of the route to the RP advertised by the assert winner; otherwise, this is zero.</td>
</tr>
<tr>
<td>Assert Winner Metric</td>
<td>If the Assert State is 'Loser', this is the routing metric of the route to the RP advertised by the assert winner; otherwise, this is zero.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; Mode field added, bidir mode support added

**Related Commands**

- `show ipv6 pim groute` Displays (S,G) state routing table entries.
**MIB Objects**

pimStarGTable
  pimStarGAddressType
  pimStarGGrpAddress
  pimStarGUptime
  pimStarGPimMode
  pimStarGRPAAddressType
  pimStarGRPAAddress
  pimStarGPimModeOrigin
  pimStarGRIPisLocal
  pimStarGUpstreamJoinState
  pimStarGUpstreamJoinTimer
  pimStarGUpstreamNeighborType
  pimStarGUpstreamNeighbor
  pimStarGRPFIfIndex
  pimStarGRPFNextHopType
  pimStarGRPFNextHop
  pimStarGRPFRouteProtocol
  pimStarGRPFRouteAddress
  pimStarGRPFRoutePrefixLength
  pimStarGRPFRouteMetricPref
  pimStarGRPFRouteMetric

pimStarGItable
  pimStarGIIfIndex
  pimStarGIUptime
  pimStarGLocalMembership
  pimStarGJoinPruneState
  pimStarGPrunePendingTimer
  pimStarGJoinExpiryTimer
  pimStarGassertState
  pimStarGassertTimer
  pimStarGassertWinnerAddressType
  pimStarGassertWinnerAddress
  pimStarGassertWinnerMetricPref
  pimStarGassertWinnerMetric
show ipv6 pim sgroute

Displays (S,G) routing table entries for IPv6 PIM.

**show ipv6 pim sgroute [source_address group_address]**

### Syntax Definitions

- **source_address**: The IPv6 address for a specific multicast source.
- **group_address**: A IPv6 multicast address.

### Defaults

By default, entire (S,G) routing table is displayed. To view the detailed information for a particular (S,G) entry, use the *source_address* and *group_address* associated with that entry.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When the *source_address* and *group_address* is specified in the command line, the detailed information displayed also includes the detailed state of every outgoing interface.
- If an IPv6 address is not specified, the current PIM status for all multicast route entries are displayed.

### Examples

```
-> show ipv6 pim sgroute

Legend: Flags: D = Dense, S = Sparse, s = SSM Group,
        L = Local, R = RPT, T = SPT, F = Register,
        P = Pruned, O = Originator

Total 1 (S,G)

Source Address       Group Address       RPF Interface   UpTime      Flags
-------------------------------+----------------+-------------+-------------+------
8ffe::3               ff0e::7          00h:01m:34s   SR

-> show ipv6 pim sgroute 8ffe::3 ff0e::7

(8ffe::3,ff0e::7)
  UpTime               = 00h:01m:40s
  PIM Mode             = ASM,
  Upstream Join State  = Not Joined,
```
Upstream RPT State     = Not Pruned,
Upstream Join Timer    = 00h:00m:00s,
Upstream Neighbor      = none,
SPT Bit                = False,
DR Register State      = No Info,
DR Register Stop Timer = 00h:00m:00s,

Interface Specific State:
  vlan-3
    UpTime       = 00h:01m:40s,
    Local Membership = False,
    Join/Prune State = No Info,
    RPT State    = No Info,
    Prune Pending Timer = 00h:00m:00s,
    Join Expiry Timer = 00h:00m:00s,
    Assert State = No Info,
    Assert Timer = 00h:00m:00s,
  vlan-4
    UpTime       = 00h:00m:00s,
    Local Membership = False,
    Join/Prune State = No Info,
    RPT State    = No Info,
    Prune Pending Timer = 00h:00m:00s,
    Join Expiry Timer = 00h:00m:00s,
    Assert State = No Info,
    Assert Timer = 00h:00m:00s,
  vlan-5
    UpTime       = 00h:00m:00s,
    Local Membership = False,
    Join/Prune State = No Info,
    RPT State    = No Info,
    Prune Pending Timer = 00h:00m:00s,
    Join Expiry Timer = 00h:00m:00s,
    Assert State = No Info,
    Assert Timer = 00h:00m:00s,

output definitions

Source-address         The IPv6 Source address.
Group-address          The IPv6 Multicast Group Address.
RPF Interface          The RPF interface towards the RP. The ifIndex is converted to the if-
                        name for the display.
Upstream Neighbor      The primary address of the neighbor on the RPF Interface that the local
                        router is sending periodic (S,G) join messages to.
UpTime                 The time since this entry was created.
Flags                  Flags indicating SPTBit, Prune State, Join State, etc.
Pim Mode                Whether the Group Address is SSM, ASM or DM.
Upstream Join State    Whether the local router should join the SPT for the source and group
                        represented by this entry.
Upstream Join Timer    The time remaining before the local router next sends a periodic (S,G)
                        Join message.
RPF Next Hop           The address of the RPF next hop towards the source.
RPF Route Protocol     The routing mechanism through which the route used to find the RPF
                        Interface towards the source was learned.
<table>
<thead>
<tr>
<th><strong>output definitions (continued)</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RPF Route Address/Prefix Length</strong></td>
<td>The IP address which when combined with the Route Prefix length identifies the route used to find the RPF interface towards the source.</td>
</tr>
<tr>
<td><strong>RPF Route Metric Pref</strong></td>
<td>The metric preference of the route used to find the RPF interface towards the source.</td>
</tr>
<tr>
<td><strong>RPF Route Metric</strong></td>
<td>The metric preference of the route used to find the RPF interface towards the source.</td>
</tr>
<tr>
<td><strong>DR Register State</strong></td>
<td>Whether the local router should encapsulate (S,G) data packets in Register messages and send them to the RP. The possible values include No Info, Join, Join Pending, or Prune.</td>
</tr>
<tr>
<td><strong>DR Register Stop Timer</strong></td>
<td>The value of the Register Stop Timer. If the Register State is 'prune', this is the time remaining before the local router sends a Null-Register message to the RP. If the State is 'joinPending', this is the time remaining before the local router resumes encapsulating data packets and sending them to the RP.</td>
</tr>
<tr>
<td><strong>Upstream Prune State</strong></td>
<td>Whether the local router has pruned itself from the tree. This is only used by PIM-DM. The possible values include forwarding, Ack Pending, or Pruned.</td>
</tr>
<tr>
<td><strong>Upstream Prune Limit Timer</strong></td>
<td>The time remaining before the local router may send a (S,G) prune message on alaPimSGRPFIfIndex. This is only used by PIM-DM.</td>
</tr>
<tr>
<td><strong>Originator State</strong></td>
<td>Whether this router is an originator for the (S,G) message flow. This is only used by PIM-DM. The possible values include Not Originator or Originator.</td>
</tr>
<tr>
<td><strong>Source Active Timer</strong></td>
<td>If this router is the Originator, this is the time remaining before the local router reverts to notOriginator state. Otherwise, this is zero. This is only used by PIM-DM.</td>
</tr>
<tr>
<td><strong>State Refresh Timer</strong></td>
<td>If Originator state is 'originator', this is the time remaining before the local router sends a State Refresh Message. Otherwise, this is zero. This is only used by PIM-DM.</td>
</tr>
<tr>
<td><strong>Interface Name</strong></td>
<td>The interface name corresponding to the ifIndex that corresponds to this entry.</td>
</tr>
<tr>
<td><strong>Uptime</strong></td>
<td>The time since this entry was created.</td>
</tr>
<tr>
<td><strong>Local Membership</strong></td>
<td>Whether the local router has (S,G) local membership on this interface.</td>
</tr>
<tr>
<td><strong>Join Prune State</strong></td>
<td>The state resulting from (S,G) Join/Prune messages received on this interface. The possible values include No Info, Join, or Prune Pending.</td>
</tr>
<tr>
<td><strong>Prune Pending Timer</strong></td>
<td>The time remaining before the local router acts on an (S,G) Prune message received on this interface, during which the router is waiting to see whether another downstream router will override the Prune message.</td>
</tr>
<tr>
<td><strong>Join Expiry Timer</strong></td>
<td>The time remaining before (S,G) Join state for this interface expires.</td>
</tr>
<tr>
<td><strong>Assert State</strong></td>
<td>The (S,G) Assert state for this interface. The possible values include No Info, Winner, or Loser.</td>
</tr>
<tr>
<td><strong>Assert Timer</strong></td>
<td>If Assert State is Winner, this is the time remaining before the local router sends a (S,G) Assert message on this interface. If the Assert State is Loser, this is the time remaining before the (S,G) Assert state expires.</td>
</tr>
<tr>
<td><strong>Assert Winner</strong></td>
<td>If the Assert State is Loser, this is the address of the assert winner.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Assert Winner Metric Pref</th>
<th>If the Assert State is Loser, this is the metric preference of the route to the source advertised by the assert winner.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assert Winner Metric Metric</td>
<td>If the Assert State is Loser, this is the routing metric of the route to the source advertised by the assert winner.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

show ipv6 pim groute Displays (*,G) routing table entries for IPv6 PIM.

**MIB Objects**

pimSGTable
  pimSGAddressType
  pimSGGrpAddress
  pimSGSrcAddress
  pimSGUpTime
  pimSGPimMode
  pimSGUpstreamJoinState
  pimSGUpstreamJoinTimer
  pimSGUpstreamNeighbor
  pimSGRPFIfIndex
  pimSGRPFNextHopType
  pimSGRPFNextHop
  pimSGRPFRouteProtocol
  pimSGRPFRouteAddress
  pimSGRPFRoutePrefixLength
  pimSGRPFRouteMetricPref
  pimSGRPFRouteMetric
  pimSGSPTBit
  pimSGKeepaliveTimer
  pimSGDRRegisterState
  pimSGDRRegisterStopTimer
  pimSGR_addressType
  pimSGRMBRAddress
  pimSGUpstreamPruneState
  pimSGUpstreamPruneLimitTimer
  pimSGOriginatorState
  pimSGSourceActiveTimer
  pimSGStateRefreshTimer

pimSGITable
  pimSGIIIfIndex
  pimSGIUpTime
  pimSGILocalMembership
  pimSGIJoinPruneState
  pimSGIJoinPendingTimer
  pimSGIJoinExppiryTimer
  pimSGIAppState
  pimSGIAssertTimer
  pimSGIAssertWinnerAddressType
  pimSGIAssertWinnerAddress
  pimSGIAssertWinnerMetricPref
  pimSGIAssertWinnerMetric
**show ipv6 pim df-election**

Displays the Designated Forwarder (DF) election state for Rendezvous Point (RP) interfaces. This command applies only to RPs operating in the Bidirectional PIM (BIDIR-PIM) mode.

```
show ipv6 pim df-election [rp_address | if_name]
```

**Syntax Definitions**

- `rp_address`: An IPv6 RP address.
- `if_name`: The interface name.

**Defaults**

By default, the DF election state for all RP interfaces.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

- When the `rp_address` is specified in the command line, only those interfaces associated with the specified RP address are displayed.
- When the `if_name` is specified in the command line, only information associated with the specified interface is displayed.

**Examples**

```
-> show ipv6 pim df-election
RP Address   Interface Name   DF State  Winner Address  Uptime       Metric  Metric Expires
-------------------------------+---------+--------+-------------------------------+-------------+-------------+-------------+
2000::8       vlan-13          Win      fe80::220:daff:fe11:2233  00h:10m:15s  1            00h:00m:13s
2000::8       vlan-210         Win      fe80::220:daff:fe11:2233  00h:10m:15s  1            00h:00m:13s
2100::8       vlan-13          Win      fe80::220:daff:fe11:2233  00h:10m:15s  1            00h:00m:03s
2100::8       vlan-210         Win      fe80::220:daff:fe11:2233  00h:10m:15s  1            00h:00m:03s

-> show ipv6 pim df-election 2000::8
RP Address   Interface Name   DF State  Winner Address  Uptime       Metric  Metric Expires
-------------------------------+---------+--------+-------------------------------+-------------+-------------+-------------+
2000::8       vlan-13          Win      fe80::220:daff:fe11:2233  00h:10m:15s  1            00h:00m:13s
2000::8       vlan-210         Win      fe80::220:daff:fe11:2233  00h:10m:15s  1            00h:00m:13s
```
show ipv6 pim df-election vlan-13

<table>
<thead>
<tr>
<th>RP Address</th>
<th>Interface Name</th>
<th>DF State</th>
<th>Winner Address</th>
<th>Uptime</th>
<th>Metric</th>
<th>Metric Expires</th>
<th>Metric Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000::8</td>
<td>vlan-13</td>
<td>Win</td>
<td>fe80::220:daff:fe11:2233</td>
<td>00h:10m:15s</td>
<td>1</td>
<td>00h:00m:13s</td>
<td></td>
</tr>
<tr>
<td>2100::8</td>
<td>vlan-13</td>
<td>Win</td>
<td>fe80::220:daff:fe11:2233</td>
<td>00h:10m:15s</td>
<td>1</td>
<td>00h:00m:03s</td>
<td></td>
</tr>
</tbody>
</table>

**Output definitions**

- **RP Address**: The IPv6 address of the Rendezvous Point (RP).
- **Interface Name**: The name of the IPv6 interface.
- **DF State**: The state of the DF election process (*Offer, Lose, Win,* or *Backoff*).
- **Winner Address**: The primary IPv6 address of the winner of the DF election process.
- **UpTime**: The amount of time since the current winner was last elected the DF for the RP.
- **Metric Pref**: The metric preference advertised by the DF winner. This value is zero if there currently is no DF.
- **Metric**: The metric value advertised by the DF winner. This value is zero if there currently is no DF.
- **Expires**: The minimum time remaining before the local router expires the current DF state.

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `show ipv6 pim interface` Displays detailed PIM settings for a specific interface.

**MIB Objects**

- `pimBidirDFElectionTable`
- `pimBidirDFElectionAddressType`
- `pimBidirDFElectionRPAddress`
- `pimBidirDFElectionIfIndex`
- `pimBidirDFElectionWinnerAddressType`
- `pimBidirDFElectionWinnerAddress`
- `pimBidirDFElectionWinnerUpTime`
- `pimBidirDFElectionWinnerMetricPref`
- `pimBidirDFElectionWinnerMetric`
- `pimBidirDFElectionState`
- `pimBidirDFElectionStateTimer`
This chapter describes multicast routing commands. Multicast routing is used in conjunction with IP Multicast Switching (IPMS). IPMS can operate either with or without multicast routing. However, for multicast routing to function, IPMS must be configured.

Multicast uses Class D IP addresses in the range 224.0.0.0 to 239.255.255.255. Addresses in the range 239.0.0.0 to 239.255.255.255 are reserved for boundaries, which are used to prevent multicast traffic from being forwarded on a VLAN group or network.

IP multicast routing is a way of controlling multicast traffic across networks. The multicast router discovers which networks want to receive multicast traffic by sending out Internet Group Management Protocol (IGMP) queries and receiving IGMP reports from attached networks. The IGMP reports signal that users want to join or leave a multicast group. If there is more than one multicast router in the network, the router with the lowest IP address is elected the querier router, which is responsible for querying the subnetwork for group members.

The current release also provides support for IPv6 multicast addresses. In the IPv6 addressing scheme, multicast addresses begin with the prefix ff00::/8. Similar to IPv6 unicast addresses, IPv6 multicast addresses also have different scopes depending on their prefix, though the range of possible scopes is different.

Multicast Listener Discovery (MLD) is the protocol used by an IPv6 router to discover the nodes which request multicast packets on its directly attached links and the multicast addresses that are of interest to those neighboring nodes. MLD is derived from version 2 of IPv4's Internet Group Management Protocol, IGMPv2. MLD uses ICMPv6 message types, rather than IGMP message types.

MIB information for the multicast routing commands is as follows:

Filename:  ALCATEL-IND1-IPMRM-MIB.mib  
Module:  alcatelIND1IPMRMIB

Filename:  IPMCAST-MIB.mib  
Module:  ipMcastMIB
A summary of the available commands is listed here:

```
ip mroute-boundary
ip mroute-boundary extended
ip mroute interface ttl
ip mroute mbr
show ip mroute-boundary
show ip mroute
show ip mroute interface
show ip mroute-nexthop
show ip mroute mbr
ipv6 mroute interface ttl
show ipv6 mroute
show ipv6 mroute interface
show ipv6 mroute-nexthop
```
### ip mroute-boundary

Adds or deletes scoped multicast address boundaries for a router interface. When a user on the specified interface joins the multicast group as defined by the scoped address—plus the mask length—all multicast traffic will stop being forwarded on that interface. This provides a mechanism for the end user to control multicast traffic from the network.

Refer to the “Configuring Multicast Address Boundaries” chapter in the *OmniSwitch AOS Release 8 Advanced Routing Configuration Guide* for detailed information.

```
ip mroute-boundary if_name scoped_address mask

no ip mroute-boundary if_name scoped_address mask
```

**Syntax Definitions**

- `if_name`:
  The interface name on which the boundary is being assigned.

- `scoped_address`:
  A scoped multicast address identifying the group range for the boundary. Scoped addresses may range from 239.0.0.0–239.255.255.255.

- `mask`:
  A corresponding Class A, B, or C mask address (e.g., 255.0.0.0).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to delete the scoped multicast address boundaries for a router interface.

**Examples**

```
-> ip mroute-boundary vlan-2 239.0.0.0 255.0.0.0
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show ip mroute-boundary  Displays scoped multicast address boundaries for the switch’s router interfaces.

MIB Objects

ipMcastBoundaryTable
  ipMcastBoundaryIfIndex
  ipMcastBoundaryAddressType
  ipMcastBoundaryAddress
  ipMcastBoundaryAddressPrefixLength
**ip mroute-boundary extended**

Enables or disables the multicast route boundary expansion feature. On enabling the multicast route boundary is extended to all the multicast groups (that is, the non-scoped address, 224.0.0.0 to 239.255.255.255). All multicast traffic will stop being forwarded on that interface. This provides a mechanism for the end user to control multicast traffic from the network.

Refer to the “Configuring Multicast Address Boundaries” chapter in the applicable OmniSwitch AOS Release 8 Advanced Routing Configuration Guide for detailed information.

**ip mroute-boundary extended {enable | disable}**

**Syntax Definitions**

- **enable**
  - The multicast route boundary is extended to all the multicast cast address groups (224.0.0.0 through 239.255.255.255).

- **disable**
  - The multicast route boundary is limited to administratively scoped multicast address (239.0.0.0 through 239.255.255.255).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- -> ip mroute-boundary extended enable
- -> ip mroute-boundary extended disable

**Release History**

Release 8.2.1; command introduced.
Related Commands

show ip mroute-boundary  Displays multicast address boundaries for the switch’s router interfaces.

MIB Objects

alaIpmrmGlobalConfig
alaIpmrmExtendedBoundaryStatus
**ip mroute interface ttl**

Specifies a multicast datagram Time to Live (TTL) threshold for an existing router interface. IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out of the interface.

**ip mroute interface if_name ttl threshold**

### Syntax Definitions

- **if_name**: The interface name that has one of the Multicast routing protocols running (either DVMRP or PIM).
- **threshold**: The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded on the interface.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> ip mroute interface vlan-1 ttl 255
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show ip mroute interface` Displays IP multicast interface information.

### MIB Objects

- `alaIpMcastInterfaceTable`  
  - `alaIpMcastInterfaceIfIndex`
Multicast Routing Commands

ip mroute interface ttl

alaIpMcastInterfaceTtl
ip mroute mbr

Configures the switch to serve as a Multicast Border Router (MBR) that will provide interoperability between DVMRP and PIM domains.

ip mroute mbr admin-state {enable | disable}

Syntax Definitions

enable

Enables MBR functionality on the switch.

disable

Disables MBR functionality on the switch.

Defaults

MBR functionality is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- To configure the switch to operate as an MBR, first configure the DVMRP and PIM protocols for the switch then enable MBR functionality.

- The MBR functionality is operationally enabled only when there is at least one PIM interface and one DVMRP interface enabled and both interfaces are operationally active on the switch.

- The MBR feature only supports interoperability between DVMRP and PIM (includes PIM-DM and PIM-SM) domains; no other routing protocols are supported.

- The following is not supported by the MBR feature in the current release:
  - PIM-SSM
  - Interoperability between multiple PIM domains
  - IPv6 (only IPv4)

Examples

- ip mroute mbr admin-state enable
- ip mroute mbr admin-state disable

Release History

Release 7.3.2; command was introduced.
Related Commands

`show ip mroute mbr`  Displays MBR configuration information.

MIB Objects

`alaIprrmMbrStatus`
**ipv6 mroute interface ttl**

Specifies a multicast datagram Time to Live (TTL) threshold for an existing IPv6 interface. Any IP multicast datagrams with a TTL value lower than the specified TTL threshold value will not be forwarded out of the interface.

```
ipv6 mroute interface if_name ttl threshold
```

**Syntax Definitions**

- `if_name`: The name of the IPv6 interface.
- `threshold`: The TTL threshold value. Values may range from 0–255. The default value of 0 allows all multicast packets to be forwarded out of the interface.

** Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900 X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> ipv6 mroute interface vlan-1 ttl 255
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show ipv6 mroute interface*  
Displays IPv6 multicast interface information.

**MIB Objects**

*alaIpMcastInterfaceTable*  
*alaIpMcastInterfaceIfIndex*  
*alaIpMcastInterfaceTtl*
show ip mroute-boundary

Displays scoped multicast address boundaries for the switch’s router interfaces.

show ip mroute-boundary

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples

-> show ip mroute-boundary
Extended Boundary Address Range: enabled

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>Interface Address</th>
<th>Boundary Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-4</td>
<td>214.0.0.7</td>
<td>239.1.1.1/32</td>
</tr>
<tr>
<td>vlan-2</td>
<td>170.2.0.1</td>
<td>224.2.2.2/24</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Extended Boundary Address Range</th>
<th>Displays the status of extended multicast route boundary on the interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>The name of the interface on which the boundary is assigned. Packets with a destination address in the associated address/mask range will not be forwarded from this interface.</td>
</tr>
<tr>
<td>Interface Address</td>
<td>The IP address of this interface where the boundary is assigned.</td>
</tr>
<tr>
<td>Boundary Address</td>
<td>The scoped multicast address that, when combined with the boundary mask, identifies the scoped boundary range. The boundary’s subnet mask is shown using the CIDR prefix length: 255.0.0.0 equals /8; 255.255.0.0 equals /16; 255.255.255.0 equals /24.</td>
</tr>
</tbody>
</table>
Release History

Release 7.1.1; command was introduced.
Release 8.2.1; Extended Boundary Address Range output field added.

Related Commands

- **ip mroute-boundary**: Adds or deletes a router’s scoped multicast address boundaries.
- **ip mroute interface ttl**: Enables or disables the multicast route boundary expansion feature.
- **show ip mroute interface**: Displays IP multicast interface information.

MIB Objects

- **ipMcastBoundaryTable**
  - ipMcastBoundaryIfIndex
  - ipMcastBoundaryAddressType
  - ipMcastBoundaryAddress
  - ipMcastBoundaryAddressPrefixLength
  - ipMcastBoundaryStatus
- **alaIpmrmGlobalConfig**
  - alaIpmrmExtendedBoundaryStatus
**show ip mroute**

Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> show ip mroute`

```
Total 2 Mroutes
Group Address  Src Address  Upstream Nbr  Route Address  Proto
----------------+-----------------+---------------+----------------+----------
225.0.0.0       214.0.0.2/32      0.0.0.0       214.0.0.0/24        PIM-SM
225.0.0.1       214.0.0.2/32      0.0.0.0       214.0.0.0/24        PIM-DM
```

**output definitions**

- **Group Address**: The IP multicast group address for this entry.
- **Src Address**: The network address which identifies the source for this entry.
- **Upstream Nbr**: The address of the upstream neighbor from which IP datagrams from these sources to this multicast address are received.
- **Route Address**: The address portion of the route used to find the upstream or parent interface for this multicast forwarding entry.
- **Proto**: The multicast routing protocol through which this multicast forwarding entry was learned (i.e., DVMRP, PIM-SM or PIM-DM).
Release History

Release 7.1.1; command was introduced.

Related Commands

- `show ip mroute interface`  Displays IP multicast interface information.
- `show ip mroute-nexthop`  Displays IP next-hop information on outgoing interfaces for routing IP multicast datagrams.

MIB Objects

```
alaIpMcastRouteTable
    alaIpMcastRouteGroup
    alaIpMcastRouteSource
    alaIpMcastRouteInIfIndex
    alaIpMcastRouteUpstreamNeighbor
    alaIpMcastRouteRtAddress
    alaIpMcastRouteRtPrefixLength
    alaIpMcastRouteProtocol
```
show ipv6 mroute

Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.

show ipv6 mroute

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 mroute
Total 2 Mroutes
Group Address Source Address Interface Upstream Neighbor Route Addr/Prefix Len Proto
---------------------------------------------------------------
ff06::7777::1 2600::7         vlan-30  fe80::2d0:95ff:feac:a537 2600::/64     PIM-SM
ff06::7777::2 2600::7         vlan-30  fe80::2d0:95ff:feac:a537 2600::/64     PIM-SM

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The IPv6 multicast group address for this entry.</td>
</tr>
<tr>
<td>Source Address</td>
<td>The IPv6 multicast address, which identifies the source for this entry.</td>
</tr>
<tr>
<td>Interface</td>
<td>The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.</td>
</tr>
<tr>
<td>Upstream Neighbor</td>
<td>The IPv6 address of the upstream neighbor from which the datagrams from these sources to this multicast address are received.</td>
</tr>
<tr>
<td>Route Addr/Prefix len</td>
<td>The IPv6 address portion of the route used to find the upstream or parent interface for this IPv6 multicast forwarding entry.</td>
</tr>
<tr>
<td>Proto</td>
<td>The IPv6 multicast routing protocol through which this IPv6 multicast forwarding entry was learned.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show ipv6 mroute interface**
  Displays IPv6 multicast interface information.

- **show ipv6 mroute-nexthop**
  Displays IPv6 next-hop information on outgoing interfaces for routing IPv6 multicast datagrams.

**MIB Objects**

alaIpMcastRouteTable
  - alaIpMcastRouteGroup
  - alaIpMcastRouteSource
  - alaIpMcastRouteInIfIndex
  - alaIpMcastRouteUpstreamNeighbor
  - alaIpMcastRouteRtAddress
  - alaIpMcastRouteRtPrefixLength
  - alaIpMcastRouteProtocol
show ip mroute interface

Displays IP multicast interface information.

show ip mroute interface [interface_name]

Syntax Definitions

interface_name

The name of the interface

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Not specifying an interface name displays all known IP multicast interfaces information.

Examples

-> show ip mroute interface

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>IP Address</th>
<th>TTL</th>
<th>Multicast Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-4</td>
<td>214.0.0.7</td>
<td>0</td>
<td>PIM</td>
</tr>
<tr>
<td>vlan-26</td>
<td>172.21.63.7</td>
<td>0</td>
<td>PIM</td>
</tr>
<tr>
<td>vlan-11</td>
<td>212.61.11.7</td>
<td>0</td>
<td>PIM</td>
</tr>
</tbody>
</table>

Output Definitions

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>The name configured for the interface.</th>
</tr>
</thead>
</table>
| IP Address             | The IP address of this interface entry.
| TTL                    | The datagram TTL threshold for the interface. Any IP multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out of the interface. The default value, 0, specifies that all multicast packets are forwarded out of the interface. |
| Multicast Protocol     | The multicast routing protocol currently running on this interface. Options include DVMRP and PIM. |
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show ip mroute**
  
  Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

- **show ip mroute-nexthop**
  
  Displays IP next-hop information on outgoing interfaces for routing IP multicast datagrams.

**MIB Objects**

- **alaIpMcastInterfaceTable**
  
  - **alaIpMcastInterfaceIfIndex**
  - **alaIpMcastInterfaceTtl**
  - **alaIpMcastInterfaceProtocol**
show ipv6 mroute interface

Displays IPv6 multicast interface information.

show ipv6 mroute interface {interface_name}

### Syntax Definitions

*interface_name*  
The name of the interface

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Not specifying an interface name displays all known IPv6 multicast interfaces information.

### Examples

```
-> show ipv6 mroute interface

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>IP Address</th>
<th>TTL</th>
<th>Multicast Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-4</td>
<td>2000::1</td>
<td>0</td>
<td>PIM</td>
</tr>
<tr>
<td>vlan-26</td>
<td>2000::2</td>
<td>0</td>
<td>PIM</td>
</tr>
<tr>
<td>vlan-11</td>
<td>2000::3</td>
<td>0</td>
<td>PIM</td>
</tr>
</tbody>
</table>
```

### output definitions

<table>
<thead>
<tr>
<th><strong>Interface Name</strong></th>
<th>The name configured for the IPv6 interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Address</strong></td>
<td>The IPv6 address of this interface entry.</td>
</tr>
<tr>
<td><strong>TTL</strong></td>
<td>The datagram TTL threshold for the interface. Any IPv6 multicast datagrams with a TTL less than the threshold displayed in the table will not be forwarded out of the interface. The default value, 0, specifies that all multicast packets are forwarded out of the interface.</td>
</tr>
<tr>
<td><strong>Multicast Protocol</strong></td>
<td>The multicast routing protocol currently running on this interface. Options include DVMRP and PIM.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show ipv6 mroute` Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.
- `show ipv6 mroute-nexthop` Displays IPv6 next-hop information on outgoing interfaces for routing IPv6 multicast datagrams.

**MIB Objects**

- `alaIpMcastInterfaceTable`
  - `alaIpMcastInterfaceIfIndex`
  - `alaIpMcastInterfaceTtl`
  - `alaIpMcastInterfaceProtocol`
**show ip mroute-nexthop**

Displays next-hop information on outgoing interfaces for routing IP multicast datagrams.

```plaintext
show ip mroute-nexthop
```

### Syntax Definitions

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
</tr>
<tr>
<td>6900</td>
<td>6900</td>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V72/C32</td>
<td>X48C6/T48C6/</td>
<td>X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>C32E/T24C2/</td>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

N/A

### Examples

```
-> show ip mroute-nexthop
Total 10 Nexthops
```

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Src Address</th>
<th>Interface Name</th>
<th>Next Hop Address</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.0.0.0</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.0</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.1</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.1</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.2</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.2</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.3</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.3</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.4</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.4</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.5</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.5</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.6</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.6</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.7</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.7</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.8</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.8</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>225.0.0.9</td>
<td>214.0.0.2/32</td>
<td>vlan-26</td>
<td>225.0.0.9</td>
<td>PIM-SM</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Group Address</th>
<th>The IP multicast group address for this entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src Address</td>
<td>The network address, which identifies the source for this entry.</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 35-23
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**show ip mroute**

Displays multicast routing information for IP datagrams sent by particular sources to the IP multicast groups known to this router.

**show ip mroute interface**

Displays IP multicast interface information.

**MIB Objects**

alaIpMcastRouteNextHopTable

- alaIpMcastRouteNextHopGroup
- alaIpMcastRouteNextHopSource
- alaIpMcastRouteNextHopIfIndex
- alaIpMcastRouteNextHopAddress
- alaIpMcastRouteNextHopProtocol

---

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Generally, this is the name configured for the interface.</td>
</tr>
<tr>
<td>Next Hop Address</td>
<td>The address of the next-hop that is specific to this entry.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The routing protocol by which this next-hop was learned (i.e., DVMRP or PIM-SM).</td>
</tr>
</tbody>
</table>
show ipv6 mroute-nexthop

Displays IPv6 next-hop information on outgoing interfaces for routing IPv6 multicast datagrams.

show ipv6 mroute-nexthop

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ipv6 mroute-nexthop
Total 2 Nexthops

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Interface</th>
<th>Next Hop Address</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>ff06:7777::1</td>
<td>2600::7</td>
<td>vlan-40</td>
<td>ff06:7777::1</td>
<td>PIM-SM</td>
</tr>
<tr>
<td>ff06:7777::2</td>
<td>2600::7</td>
<td>vlan-40</td>
<td>ff06:7777::2</td>
<td>PIM-SM</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>The IPv6 multicast group address for this entry.</td>
</tr>
<tr>
<td>Src Address</td>
<td>The IPv6 multicast address, which identifies the source for this entry.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The name of the IPv6 interface on which the datagrams sent by these sources to this IPv6 multicast address are received.</td>
</tr>
<tr>
<td>Next Hop Address</td>
<td>The IPv6 address of the next-hop that is specific to this entry.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The IPv6 multicast routing protocol by which this IPv6 multicast forwarding entry was learned.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Related Commands

- **show ipv6 mroute**
  Displays multicast routing information for IPv6 datagrams sent by particular sources to the IPv6 multicast groups known to this router.

- **show ipv6 mroute interface**
  Displays IPv6 multicast interface information.

MIB Objects

alaIpMcastRouteNextHopTable
  - alaIpMcastRouteNextHopGroup
  - alaIpMcastRouteNextHopSource
  - alaIpMcastRouteNextHopIfIndex
  - alaIpMcastRouteNextHopAddress
  - alaIpMcastRouteNextHopProtocol
show ip mroute mbr

Displays the MBR status for the switch.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The MBR feature only supports interoperability between DVMRP and PIM. Both of these multicast protocols must be configured and operationally active on the switch.

Examples

```
-> show ip mroute mbr
MBR Status               = enabled,
Protocols Registered     = DVMRP PIM
```

output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MBR Status</td>
<td>The administrative status (<code>enabled</code> or <code>disabled</code>) of MBR functionality</td>
</tr>
<tr>
<td></td>
<td>on the switch.</td>
</tr>
<tr>
<td>Protocols Registered</td>
<td>The operationally active multicast protocols (<code>DVMRP</code>, <code>PIM</code>) to which MBR</td>
</tr>
<tr>
<td></td>
<td>functionality is applied.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command was introduced.
Related Commands

*ip mroute mbr*  
Configures the administrative status of Multicast Border Router functionality.

MIB Objects

*alaIpmrmGlobalConfig*
*alaIpmrmMbrStatus*
*alaIpmrmMbrProtocolApps*
36  QoS Commands

The OmniSwitch QoS software provides a way to manipulate flows coming through the switch based on user-configured policies. The flow manipulation (generally referred to as Quality of Service or QoS) may be as simple as allowing/denying traffic, or as complicated as remapping 802.1p bits from a Layer 2 network to ToS values in a Layer 3 network.

This chapter provides information about configuring QoS global and port parameters through the Command Line Interface (CLI). Refer to Chapter 44, “QoS Policy Commands,” for information about commands used to configure QoS policy rules.

MIB information for the QoS commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-QOS-MIB.mib</td>
<td>alaQoSMIB</td>
</tr>
<tr>
<td>ALCATEL-IND1-VIRTUAL-FLOW-CONTROL-MIB.mib</td>
<td>alcatelIND1VfcMIB</td>
</tr>
</tbody>
</table>

Some of the commands listed here are not currently supported on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS commands are listed here:

<table>
<thead>
<tr>
<th>Global commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos</td>
</tr>
<tr>
<td>qos trust-ports</td>
</tr>
<tr>
<td>qos forward log</td>
</tr>
<tr>
<td>qos log console</td>
</tr>
<tr>
<td>qos log lines</td>
</tr>
<tr>
<td>qos log level</td>
</tr>
<tr>
<td>qos stats interval</td>
</tr>
<tr>
<td>qos phones</td>
</tr>
<tr>
<td>qos quarantine mac-group</td>
</tr>
<tr>
<td>qos user-port</td>
</tr>
<tr>
<td>qos dei</td>
</tr>
<tr>
<td>debug qos</td>
</tr>
<tr>
<td>debug qos internal</td>
</tr>
<tr>
<td>clear qos log</td>
</tr>
<tr>
<td>qos apply</td>
</tr>
<tr>
<td>qos revert</td>
</tr>
<tr>
<td>qos flush</td>
</tr>
<tr>
<td>qos reset</td>
</tr>
<tr>
<td>qos stats reset</td>
</tr>
<tr>
<td>qos switch-group</td>
</tr>
<tr>
<td>show qos slice</td>
</tr>
<tr>
<td>show qos log</td>
</tr>
<tr>
<td>show qos config</td>
</tr>
<tr>
<td>show qos statistics</td>
</tr>
</tbody>
</table>
### QoS Commands

<table>
<thead>
<tr>
<th>Port and Slice commands</th>
<th>qos port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>qos port reset</td>
</tr>
<tr>
<td></td>
<td>qos port trusted</td>
</tr>
<tr>
<td></td>
<td>qos port maximum egress-bandwidth</td>
</tr>
<tr>
<td></td>
<td>qos port maximum ingress-bandwidth</td>
</tr>
<tr>
<td></td>
<td>qos port maximum depth</td>
</tr>
<tr>
<td></td>
<td>qos port default 802.1p</td>
</tr>
<tr>
<td></td>
<td>qos port default dscp</td>
</tr>
<tr>
<td></td>
<td>qos port default classification</td>
</tr>
<tr>
<td></td>
<td>qos port dei</td>
</tr>
<tr>
<td></td>
<td>show qos port</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Queue Management commands</th>
<th>qos qsp import</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>qos qsp qp</td>
</tr>
<tr>
<td></td>
<td>qos qsi qos</td>
</tr>
<tr>
<td></td>
<td>qos qsp system-default</td>
</tr>
<tr>
<td></td>
<td>qos qsi stats</td>
</tr>
<tr>
<td></td>
<td>show qos qsi summary</td>
</tr>
<tr>
<td></td>
<td>show qos qsp</td>
</tr>
<tr>
<td></td>
<td>show qos wrp</td>
</tr>
<tr>
<td></td>
<td>show qos qsi</td>
</tr>
<tr>
<td></td>
<td>show qos qsi stats</td>
</tr>
<tr>
<td></td>
<td>show qos qsi ecn-stats</td>
</tr>
<tr>
<td></td>
<td>show qos qsi wred-stats</td>
</tr>
<tr>
<td></td>
<td>show qos qsp system-default</td>
</tr>
<tr>
<td></td>
<td>clear qos qsi stats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Center Bridging commands</th>
<th>qos qsp dcb import</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>qos qsp dcb tc</td>
</tr>
<tr>
<td></td>
<td>qos qsp dcb tc-numbering</td>
</tr>
<tr>
<td></td>
<td>qos qsi qos dcb</td>
</tr>
<tr>
<td></td>
<td>qos qsi dcb dcbx version</td>
</tr>
<tr>
<td></td>
<td>qos qsi dcb dcbx admin-state</td>
</tr>
<tr>
<td></td>
<td>qos qsi dcb dcbx ets</td>
</tr>
<tr>
<td></td>
<td>qos qsi dcb dcbx pfc</td>
</tr>
<tr>
<td></td>
<td>show qos qsi summary</td>
</tr>
<tr>
<td></td>
<td>show qos qsp dcb</td>
</tr>
<tr>
<td></td>
<td>show qos qsi dcb dcbx</td>
</tr>
<tr>
<td></td>
<td>show qos qsi dcb ets</td>
</tr>
<tr>
<td></td>
<td>show qos qsi dcbx pfc</td>
</tr>
<tr>
<td></td>
<td>show qos pfc-lossless-usage</td>
</tr>
<tr>
<td></td>
<td>show qos qsi dcb pfc stats</td>
</tr>
<tr>
<td></td>
<td>show qos qsi stats</td>
</tr>
<tr>
<td></td>
<td>clear qos qsi stats</td>
</tr>
<tr>
<td></td>
<td>clear qos qsi dcb pfc stats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Explicit Congestion Notification (ECN)</th>
<th>qos ecnp import ecnp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>qos ecnp value</td>
</tr>
<tr>
<td></td>
<td>qos qsp ecn-profile</td>
</tr>
<tr>
<td></td>
<td>qos qsi qp ecn</td>
</tr>
<tr>
<td></td>
<td>show qos ecnp</td>
</tr>
</tbody>
</table>
**qos**

Enables or disables QoS. This section describes the base command with a single required option (enable or disable).

In lieu of this option, the base command (qos) may be used with other keywords to set up global QoS configuration. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a no form to remove the parameter or return it to its default.

```
qos {enable | disable}
  [trust-ports]
  [forward log]
  [log console]
  [log lines lines]
  [log level level]
  [stats interval seconds]
  [phones [priority priority_value | trusted]]
  [user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}]
```

---

### Syntax Definitions

**enable**

Enables QoS. The QoS software in the switch classifies flows coming into the switch to attempt to match them to QoS policies. If a match is found, the policy parameters are applied to the flow. The enable setting may be used alone or in conjunction with optional command keywords.

**disable**

Disables QoS. Flows coming into the switch are not matched to policies. The disable setting cannot be used with any other command keyword.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

|       | 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 | 6900 | 6900 | 6900 | 6900 | 9900 |
|-------|------|------|------|-------|------|-------|------|------|------|------|------|------|------|------|------|------|
|       | Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  | Yes  |

---

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 36-3
**Usage Guidelines**

- When QoS is disabled, flows coming into the switch are classified but not matched to a policy. Traffic is treated as best effort and assigned to default queues.

- The command keywords may be used with or without `enable`; these keywords cannot be used with `disable`.

**Examples**

```
-> qos disable
-> qos enable
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos apply</td>
<td>Applies configured QoS and policy settings to the current configuration.</td>
</tr>
<tr>
<td>policy rule</td>
<td>Configures a policy rule on the switch.</td>
</tr>
<tr>
<td>show policy rule</td>
<td>Displays information for policy rules configured on the switch.</td>
</tr>
</tbody>
</table>

**MIB Objects**

alaQoSConfigTable
  - alaQoSConfigEnable
  - alaQoSConfigTrustedPorts
  - alaQoSConfigForwardLog
  - alaQoSConfigLogLines
  - alaQoSConfigLogLevel
  - alaQoSConfigLogConsole
  - alaQoSConfigStatsInterval
  - alaQoSConfigAutoPhones
  - alaQoSConfigUserportFilter
  - alaQoSConfigAppliedUserportFilter
  - alaQoSConfigUserportShutdown
  - alaQoSConfigAppliedUserportShutdown
qos trust-ports

Configures the global trust mode for QoS ports. Trusted ports can accept 802.1p and ToS/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

Any port configured through the qos port command will automatically be added in the trust mode specified by this command. See page 36-41 for more information about this command.

qos trust-ports
qos no trust-ports

Syntax Definitions

N/A

Defaults

By default, all ports are untrusted.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the qos ports trusted command to override the default for a particular port.
- The setting only applies to ports with incoming traffic.
- Mobile ports are always trusted regardless of the global setting.
- Use the qos port default 802.1p or qos port default dscp commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different value for such packets.

Examples

-> qos trust-ports
-> qos no trust-ports

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **qos port**
  Configures a physical port for QoS.
- **qos port trusted**
  Configures whether or not a particular port is trusted or untrusted.
- **show qos port**
  Displays information about QoS ports.

**MIB Objects**

- **alaQoSConfigTable**
- **alaQoSConfigTrustedPorts**
qos forward log

Enables the QoS software in the switch to send events to the policy server software in the switch in real time. The policy server software may then be polled by an NMS application for logged events.

qos forward log
qos no forward log

Syntax Definitions

N/A

Defaults

By default, logged events are not sent to the policy server software in the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

An NMS application may query the Policy Manager in the switch for logged events. Use the qos forward log command to forward each event as it happens.

Examples

--> qos forward log

Release History

Release 7.1.1; command was introduced.

Related Commands

qos log lines Configures the number of lines in the QoS log.
show qos log Displays the log of QoS events.

MIB Objects

alaQoSConfigTable
alaQoSConfigForwardLog
**qos log console**

Sends QoS log messages to the switch logging utility, which is an event logging application available on the OmniSwitch. The configuration of the switch logging utility determines if QoS messages are sent to a log file in the switch’s flash file system, displayed on the switch console, or sent to a remote syslog server.

```qos log console
qos no log console```

### Syntax Definitions

N/A

### Defaults

QoS log messages are not sent to the switch logging utility by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- To display QoS log events as they happen on an output console attached to the switch, configure the switch logging utility to output events to the console. This is done using the `swlog output` command.

- The entire log may be viewed at any time using the `show qos log` command.

### Examples

- `-> qos log console`
- `-> qos no log console`

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **qos log lines**
  Configures the number of lines in the QoS log.

- **swlog output**
  Enables or disables switch logging output to the console, file, or data socket (remote session).

- **show qos log**
  Displays the log of QoS events.

**MIB Objects**

- **alaQoSConfigTable**
  - **alaQoSConfigLogConsole**
qos log lines

Configures the number of lines in the QoS log.

qos log lines lines

Syntax Definitions

lines The number of lines included in the QoS log. A value of zero turns off logging to the console. The range is 0–10240.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>lines</td>
<td>10240</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- To turn off logging, enter 0 for the number of log lines. (Note that error messages will still be logged.)
- If you change the number of log lines, you may clear all messages in the QoS log. To avoid clearing all messages in the log, enter the qos log lines command in the boot.cfg file. The log length will be changed at the next reboot.

Examples

- > qos log lines 5
- > qos log lines 0

Release History

Release 7.1.1; command was introduced.
Related Commands

show qos log

Displays the log of QoS events.

MIB Objects

alaQoSConfigTable

alaQoSConfigLogLines
qos log level

Configures the level of log detail.

qos log level level

qos no log level

Syntax Definitions

level The level of log detail, ranging from 1 (least detail) to 8 (most detail).

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>5</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the debug qos command to change the type of debugging messages that are logged. The qos log level command configures the level of detail for these messages.

- If the debug qos command is not configured to log any kind of information (this is the default), the qos log level command has no effect.

- Note that a high log level value will impact the performance of the switch.

Examples

-> qos log level 4
-> qos log level 0

Release History

Release 7.1.1; command was introduced.
Related Commands

- `qos log lines`  Configure the number of lines in the QoS log.
- `show qos log`    Displays the log of QoS events.

MIB Objects

- `alaQoSConfigTable`  
  - `alaQoSConfigLogLevel`
**qos stats interval**

Configures how often the switch polls network interfaces for statistics about QoS events.

```plaintext
qos stats interval seconds
```

**Syntax Definitions**

`seconds` The number of seconds before the switch polls network interfaces for statistics. The range is 1–3600.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- Change the statistics interval to a smaller interval if you want to monitor QoS events.
- Change the statistics interval to a larger interval if you want to free some switch memory.

**Examples**

```plaintext
-> qos stats interval 30
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated, interval set to 5 seconds.

**Related Commands**

- `show qos statistics` Displays statistics about the QoS configuration.

**MIB Objects**

- `alaQoSCfgTable`  
  - `alaQoSCfgStatsInterval`
**qos phones**

Enables or disables the automatic prioritization of IP phone traffic.

```
qos phones [priority priority_value | trusted]
qos no phones
```

---

**Syntax Definitions**

- `priority_value`: The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).
- `trusted`: Trusts IP phone traffic; priority value of the IP phone packet is used.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>priority_value</code></td>
<td>trusted</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to disable automatic prioritization of IP phone traffic.

- IP phone traffic is identified by examining the source MAC address of the packet received on the port. If the source MAC falls within one of the following ranges, the QoS IP phone priority is automatically assigned to the MAC:

<table>
<thead>
<tr>
<th>MAC Address Range</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:80:9f:00:00:00—00:80:9f:ff:ff:ff</td>
<td>Enterprise IP Phones Range</td>
</tr>
<tr>
<td>78:81:02:00:00:00—78:81:02:ff:ff:ff</td>
<td>Communications IP Phones Range</td>
</tr>
<tr>
<td>00:13:fa:00:00:00—00:13:fa:ff:ff:ff</td>
<td>Lifesize IP Phones Range</td>
</tr>
<tr>
<td>48:7a:55:00:00:00—48:7a:55:ff:ff:ff</td>
<td>ALE 8008 IP Phone MAC Range</td>
</tr>
</tbody>
</table>

- To automatically apply the QoS IP phone priority to other, non-IP phone traffic, add the source MAC addresses of such traffic to the QoS “alaPhones” group.

- When automatic prioritization of IP phone traffic is enabled, QoS policies that specify priority are not applied to the IP phone traffic. Other QoS policies, however, are applied to this type of traffic as usual.
On the OmniSwitch 6860, consider the following:

- When automatic prioritization of QoS IP phone traffic is enabled, a rule is configured in the FFP (Fast Filtering Processor) with the source MAC address as 00:80:9F:00:00:00 and the mask FF:FF:FF:00:00:00 and 00-13-FA-xx-xx-xx and mask FF:FF:FF:00:00:00.

- The QoS IP phone prioritization and SIP Snooping features are mutually exclusive. If one of these features is enabled when an attempt is made to enable the other feature, an error message is displayed. To enable QoS IP phone prioritization, first use the `sip-snooping admin-state disable` command to disable SIP Snooping. To enable the SIP Snooping feature, first use the `qos no phones` command to disable QoS IP phone prioritization.

**Note.** QoS IP phone prioritization is configured, by default, on initialization.

### Examples

- `qos phones priority 7`
- `qos phones trusted`
- `qos no phones`

### Release History

Release 7.1.1; command was introduced.
Release 8.5R2; additional IP phone MAC ranges added.

### Related Commands

- `show qos config`
  Displays the QoS configuration for the switch.

### MIB Objects

- `alaQoSConfigTable`
- `alaQoSConfigAutoPhones`
**qos quarantine mac-group**

Configures the name of the Quarantine MAC address group. The OmniVista Quarantine Manager application identifies source MAC addresses to quarantine and adds these addresses to the Quarantine MAC group.

**qos quarantine mac-group** *mac_group*

**qos no quarantine mac-group**

---

**Syntax Definitions**

*mac_group* The name of the Quarantine MAC group (up to 31 alphanumeric characters).

---

**Defaults**

By default, the quarantine MAC group is not configured on the switch.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/C32E/T24C2/</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the *no* form of the command to reset the default MAC group name back to “Quarantined”.
- The *mac_group* name specified with this command must match the group name specified with the OmniVista Quarantine Manager application.
- Each switch can have a different Quarantine MAC group name as long as each switch matches the OmniVista Quarantine Manager MAC group name for that switch. Note that there is only one such MAC group per switch.
- Do not use the Quarantine MAC group name in regular QoS policies.
- This group is also used by the switch Quarantine Manager and Remediation (QMR) application to restrict or restore network access to quarantined MACs.
- Note that QMR is not available if VLAN Stacking services or QoS VLAN Stacking inner VLAN and 802.1p policies are configured on the switch.
- QMR is considered active when there are MAC addresses in the Quarantine MAC address group. Use the *show quarantine mac group* command to display the contents of this group. In addition, the *show mac-learning* command output display identifies quarantined MAC addresses.
Examples

-> qos quarantine mac-group mac_group1
-> no quarantine mac-group

Release History

Release 8.1.1; command was introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qmr quarantine path</td>
<td>Specifies the URL for a remediation server.</td>
</tr>
<tr>
<td>qmr quarantine page</td>
<td>Configures the Quarantine Manager and Remediation (QMR) application to send a Quarantined page to a client if a remediation server is not configured.</td>
</tr>
<tr>
<td>show quarantine mac group</td>
<td>Displays information about the Quarantine MAC group.</td>
</tr>
<tr>
<td>show qmr</td>
<td>Displays the QMR configuration for the switch.</td>
</tr>
</tbody>
</table>

MIB Objects

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaQoSConfigTable</td>
<td></td>
</tr>
<tr>
<td>alaQoSConfigQuarantineMacGroupName</td>
<td></td>
</tr>
</tbody>
</table>
qos user-port

Configures the option to filter packets or administratively disable a port when the specified type of traffic is received on a port that is a member of the pre-defined UserPorts group.

qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}

qos no user-port {filter | shutdown}

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Filters the specified type of traffic when it is received on UserPorts ports.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Administratively disables UserPorts ports that receive the specified type of traffic.</td>
</tr>
<tr>
<td>spoof</td>
<td>Detects IP spoofing. The source IP address of a packet ingressing on a user port is compared to the subnet of the VLAN/service for the user port; the packet is dropped if these two items do not match. This parameter is not supported on the OmniSwitch 6360 and OmniSwitch 6465.</td>
</tr>
<tr>
<td>bgp</td>
<td>Filters only BGP protocol packets from a TCP session that was not originated by the same switch that has this filter configured.</td>
</tr>
<tr>
<td>bpdu</td>
<td>Filters conventional Spanning Tree BPDU (destination MAC address 0x0180c2:000000) packets and GVRP (destination MAC address 0x0180c2:000021) packets.</td>
</tr>
<tr>
<td>rip</td>
<td>Filters RIP protocol packets.</td>
</tr>
<tr>
<td>ospf</td>
<td>Filters OSPF protocol packets.</td>
</tr>
<tr>
<td>vrrp</td>
<td>Filters VRRP protocol packets.</td>
</tr>
<tr>
<td>dvmrp</td>
<td>Filters IGMP packets with a type of 0x13. This applies only to IP packets with no options.</td>
</tr>
<tr>
<td>pim</td>
<td>Filters PIMv1, PIM-DM, and PIM-SM packets. The PIMv1 filter applies only to IP packets with no options.</td>
</tr>
<tr>
<td>isis</td>
<td>Filters IS-IS protocol packets.</td>
</tr>
<tr>
<td>dhcp-server</td>
<td>Filters response packets originating from a DHCP or BOOTP server that is configured on the known UDP port 67.</td>
</tr>
<tr>
<td>dns-reply</td>
<td>Filters all packets (both TCP and UDP) that originate from the known DNS port 53.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>spoof</td>
</tr>
<tr>
<td>shutdown</td>
<td>none</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to disable the filter or shutdown function. This form of the command effects the overall operation of the feature.

- To specify more than one traffic type in the same command line, enter each type separated by a space (e.g., `spoof bgp ospf`).

- The **filter** option is applied only to ingress traffic on ports that are members of the UserPorts group. However, the switch will still process the filtered packets to determine if an egress update is sent on the same port. For example, if RIP traffic is filtered, the switch will still send RIP peer updates on that port.

- Note that existing traffic types to filter or shutdown are removed each time the **filter** or **shutdown** option is configured. Specify all desired traffic types each time the **qos user-port** command is performed to retain previously configured traffic types.

- No changes to the **filtering** and **shutdown** options are applied to the switch until the **qos apply** command is performed.

- This command only applies to ports that are members of the UserPorts group. Use the **policy port group** command to create and assign members to the UserPorts group.

- An SNMP trap is sent when a port is administratively disabled through a UserPorts shutdown function or a port disable action.

- To enable a port disabled by a user port shutdown operation, use the **interfaces admin** command to administratively enable the port or disconnect and reconnect the port cable.

- Up to a fixed number of IP interfaces are supported with spoof detection on user ports. If the number of interfaces exceeds this number, user port packets ingressing on those interfaces are dropped.

- To enforce anti-spoofing, a VLAN/service must have an IP address associated with it. If there is no IP address associated with the VLAN/service, no packets will be dropped.

- Anti-spoofing on service is supported only on SPB SAP ports and is supported on OmniSwitch 6860N, and OmniSwitch 6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 where inline routing is supported.

Examples

- `-> qos user-port filter spoof bpdu`
- `-> qos user-port shutdown spoof bgp ospf`
- `-> qos no user-port shutdown`
**QoS Commands qos user-port**

**Release History**
Release 7.1.1; command was introduced.

**Related Commands**
- `policy port group` Configures a port group and its associated slot and port numbers.
- `show qos config` Displays QoS configuration information.

**MIB Objects**
- `alaQoSConfigTable`
- `alaQoSConfigUserportFilter`
- `alaQoSConfigAppliedUserportFilter`
- `alaQoSConfigUserportShutdown`
- `alaQoSConfigAppliedUserportShutdown`
**qos dei**

Configures the global Drop Eligible Indicator (DEI) bit mapping and marking setting for all QoS ports. The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) or other rate limiting mechanisms.

`qos dei {ingress | egress}`

`qos no dei {ingress | egress}`

**Syntax Definitions**

- **ingress**: Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress traffic. *DEI mapping is not supported on the OmniSwitch 6465.*
- **egress**: Marks the DEI/CFI bit for egress packets if the packets were marked yellow as a result of the rate limiting process.

**Defaults**

By default, no DEI bit marking or mapping is done.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the global DEI bit mapping (ingress) or marking (egress) configuration for the switch.
- Use the `qos port dei` command to set the DEI bit mapping and marking configuration for a specific port. Note that the port setting takes precedence over the global DEI setting.
- Packets marked yellow by rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI bit for yellow egress packets (qos dei egress) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI bit set and ingress DEI bit mapping is enabled (qos dei ingress), the packet is mapped to an internal drop precedence or yellow color marking for the switch.
- DEI bit mapping is not supported on the OmniSwitch 6465. As a result, packets are processed as follows on that switch:
  - When packets are received on a trusted port, the DEI bit is retained only if the packets were not subject to a meter. If the port is untrusted, however, the DEI bit is always reset.
  - When a meter is set and DEI egress is configured on a trusted port, the DEI bit is reset to 0 for green
packets. Yellow–red packets egress with the DEI bit set to 1.

**Examples**

- `qos dei ingress`
- `qos dei egress`
- `qos no dei ingress`
- `qos no dei egress`

**Release History**

Release 7.2.1; command was introduced.

**Related Commands**

- `qos port` Configures a physical port for QoS.
- `qos port dei` Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port.
- `policy action cir` Configures a Tri-Color Marking policy action.
- `show qos config` Displays global information about the QoS configuration.
- `show qos port` Displays information about QoS ports.

**MIB Objects**

- `alaQoSConfigTable`
  - `alaQoSConfigDEIMapping`
  - `alaQoSConfigDEIMarking`
**debug qos**

Configures the type of QoS events that will be displayed in the QoS log.

```
debug qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]
```

```
debug no qos
```

```
debug no qos [info] [config] [rule] [main] [port] [msg] [sl] [ioctl] [mem] [mapper] [slot] [l2] [l3] [classifier] [nat] [sem] [pm] [ingress] [egress]
```

---

**Syntax Definitions**

- **info**: Logs basic information about the switch.
- **config**: Logs information about the global configuration.
- **rule**: Logs events for rules configured on the switch.
- **main**: Logs information about basic program interfaces.
- **port**: Logs events related to QoS ports.
- **msg**: Logs QoS messages.
- **sl**: Logs information about source learning.
- **mem**: Logs information about memory.
- **mapper**: Logs information about mapping queues.
- **slot**: Logs events related to slots.
- **l2**: Logs Layer 2 QoS events on the switch.
- **l3**: Logs Layer 3 QoS events on the switch.
- **classifier**: Logs information whenever the switch classifies a flow; more details are provided if the log level is higher.
- **nat**: Not supported in this release.
- **sem**: Logs information about semaphore, process locking.
- **pm**: Logs events related to the Policy Manager.
- **ingress**: Logs information about packets arriving on the switch.
- **egress**: Logs information about packets leaving the switch.

**Defaults**

By default basic information messages are logged (**info**). Error messages are always logged.
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to change the type of messages that will be logged or to return debugging to its default state.
- Use this command to troubleshoot QoS events on the switch.

Examples

-> debug qos flows queue
-> qos debug no flows no queue
-> debug no qos

Release History

Release 7.1.1; command was introduced.

Related Commands

- **qos forward log** Enables the switch to send events to the PolicyView application in real time.
- **qos log lines** Configures the number of lines in the QoS log.
- **qos log level** Configures the level of log detail.
- **show qos log** Displays the log of QoS events.

MIB Objects

- **alaQoSConfigTable**
  - **alaQoSConfigDebug**
**debug qos internal**

Displays debugging information for QoS internal to the switch.

```
debug qos internal [slot/slice] [flow] [queue] [port] [l2tree] [l3tree] [vector] [pending] [verbose] [mapper] [pool] [log] [pingonly | nopingonly]
```

### Syntax Definitions

- **slot/slice**
  The slot number and slice to view debugging information. A *slice* is a logical section of hardware that corresponds to particular ports on a network interface module.

- **flow**
  Displays information about QoS flows.

- **queue**
  Displays information about QoS queues.

- **port**
  Displays information about QoS ports.

- **l2tree**
  Displays information about Layer 2 flows.

- **l3tree**
  Displays information about Layer 3 flows.

- **vector**
  Displays information about vectors.

- **pending**
  Displays information about pending QoS objects.

- **verbose**
  Sets the output to verbose mode for more detailed information.

- **mapper**
  Displays information about QoS mapping flows to queues.

- **pool**
  Displays information about the buffer pool.

- **log**
  Displays information about QoS information that is logged.

- **pingonly**
  Specifies that any policies configured with an ICMP protocol condition apply only to ICMP echo-requests and echo-replies.

- **nopingonly**
  Configures the switch so that any policies configured with an ICMP protocol condition apply to any ICMP packets.

### Defaults

Debugging is disabled by default.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>pingonly</td>
<td>nopingonly</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```
Usage Guidelines

- Use the `debug qos` command to configure the type of QoS events that will be displayed in the QoS log.
- Use the `qos log level` command to set the level of log detail in the QoS log.

Examples

`-> debug qos internal "verbose log"

Release History

Release 7.1.1; command was introduced.

Related Commands

- `debug qos` — Configures the type of QoS events that will be displayed in the QoS log.
- `qos log level` — Configures the level of log detail.

MIB Objects

N/A
**clear qos log**

Clears messages in the current QoS log.

**clear qos log**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is useful for clearing messages from a large log file so that the file is easier to view. Logs can get large if invalid rules are configured on the switch, or if a lot of QoS events have taken place. Clearing the log makes the file easier to manage.

**Examples**

`-> clear qos log`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `qos log lines` Configures the number of lines in the QoS log.
- `show qos log` Displays the log of QoS events.

**MIB Objects**

- `alaQoSConfigTable`  
  - `alaQoSConfigClearLog`
### qos apply

Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).

**qos apply**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is required to activate all QoS and policy commands. This is the only command that causes current changes to be written to flash.

- Rules are configured through the **policy rule** command, but are not active on the switch until you enter **qos apply**.

**Examples**

```bash
-> qos apply
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **qos revert**: Removes any policies configured through policy rule but not applied to the current configuration through the **qos apply** command.
- **qos reset**: Resets the QoS configuration to its default values.
- **qos flush**: Deletes all pending policy information.
### MIB Objects

<table>
<thead>
<tr>
<th>alaQoSConfigTable</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaQoSConfigApply</td>
</tr>
</tbody>
</table>
**qos revert**

Deletes any QoS configuration that has not been applied to the configuration through the `qos apply` command.

```
qos revert
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to remove currently configured policies that have not yet been activated through the `qos apply` command.

**Examples**

```
-> qos revert
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **policy rule**
  Configures a policy rule and saves it to the current configuration but does not make it active on the switch.

- **qos apply**
  Applies all QoS settings configured on the switch to the current configuration.

- **qos reset**
  Resets the QoS configuration to its defaults.

**MIB Objects**

- **alaQoSConfigTable**
  - **alaQoSConfigRevert**
**qos flush**

Deletes all pending policy information. This command is different from **qos revert**, which returns the pending policy configuration to its last applied settings.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If you enter this command, the pending policy configuration is completely erased. If you then enter **qos apply**, the erased configuration overwrites the applied policies and you will erase all of your policy configuration.

Do not use this command unless you want to erase all of your policy configuration and start configuring new policies.

- Use the **qos revert** command to return the pending policy configuration to its last applied value.

- Policy configuration includes the following commands:

```
<table>
<thead>
<tr>
<th>base commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy rule</td>
</tr>
<tr>
<td>policy network group</td>
</tr>
<tr>
<td>policy service</td>
</tr>
<tr>
<td>policy service group</td>
</tr>
<tr>
<td>policy mac group</td>
</tr>
<tr>
<td>policy port group</td>
</tr>
<tr>
<td>policy condition</td>
</tr>
<tr>
<td>policy action</td>
</tr>
</tbody>
</table>
```

**Examples**

-> qos flush

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**qos revert**
Deletes any QoS configuration that has not been applied to the configuration through the `qos apply` command.

**qos apply**
Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).

**policy server flush**
Removes all cached LDAP policy data from the switch.

MIB Objects

alaQoSConfigTable
alaQoSConfigFlush
**qos reset**

Resets the QoS configuration to its defaults.

```
qos reset
```

---

### Syntax Definitions

N/A

---

### Defaults

N/A

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

Use this command to reset QoS configuration that has not yet been applied through the `qos apply` command. The parameters are reset to their defaults.

---

### Examples

```
-> qos reset
```

---

### Release History

Release 7.1.1; command was introduced.

---

### Related Commands

- **qos apply**
  - Applies all QoS settings configured on the switch to the current configuration.

- **qos revert**
  - Deletes any QoS configuration that has not been applied to the configuration through the `qos apply` command.

---

### MIB Objects

- `alaQoSConfigTable`
- `alaQoSConfigReset`
**qos stats reset**

Resets QoS statistic counters to zero.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to reset global QoS statistics to zero. Statistics may be displayed with the `show qos statistics` command.

**Examples**

-> qos stats reset

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show qos statistics` Displays statistics about the QoS configuration.

**MIB Objects**

- `alaQoSConfigTable`  
  - `alaQoSConfigStatsReset`
qos switch-group

Changes how the switch handles IP addresses configured on the switch to help reduce the number of hardware entries required for QoS policies that use an IP address configured on the switch.

qos switch-group {expanded | compact}

Syntax Definitions

expanded
Uses the expanded method for populating the hardware routing table. This method requires a hardware entry for each individual IP interface belonging to either the built-in 'Switch' or 'Switch6' network groups.

compact
Uses the compact method for populating the hardware routing table by programming a single next hop entry for all IP interfaces belonging to either the built-in 'Switch' or 'Switch6' network groups.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>expanded</td>
<td>compact</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The expanded method can be used to reduce the hardware entries required and allow for a single hardware entry to be programmed for all the IP interfaces belonging to either the built-in 'Switch' or 'Switch6' network groups instead of a hardware entry for each individual IP address.
- The built-in policy network group 'Switch' contains all the IPv4 interfaces configured on the switch.
- The built-in policy network group 'Switch6' contains all the IPv6 interfaces configured on the switch.
- It is required to reboot the switch for the switch group setting to take effect. The current setting will always be shown, with the modified setting in parentheses in the show qos config command.

Examples

-> qos switch-group compact
-> qos switch-group expanded
**Release History**

Release 8.4.1 R02; command introduced.

**Related Commands**

- `show qos config` Displays global information about the QoS configuration.

**MIB Objects**

- `alaQoSConfig`
- `alaQoSConfigSwitchGroup`
qos port reset

Resets all QoS port configuration to the default values.

qos port chassis/slot/port[-port2] reset

Syntax Definitions

chassis The chassis identifier.
slot/port[-port2] A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Usage Guidelines

The QoS port configuration parameters that are reset include:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>default queues</td>
<td>8</td>
</tr>
<tr>
<td>trusted</td>
<td>not trusted</td>
</tr>
</tbody>
</table>

Examples

-> qos port 3/1 reset

Release History

Release 7.1.1; command was introduced.

Related Commands

show qos port Displays information about QoS ports.
**MIB Objects**

alaQoSPortTable
alaQoSPortSlot
alaQoSPortPort
alaQoSPortReset
**qos port**

Configures QoS parameters for a physical port. This section describes the base command with a single required option (slot/port).

In lieu of these options, the base command (qos port) may be used with other keywords to set up a QoS configuration on a per port basis. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a **no** form to remove the parameter or return it to its default.

```
qos port chassis/slot/port[-port2]
    [trusted]
    [maximum egress-bandwidth bps]
    [maximum ingress-bandwidth bps]
    [maximum {ingress | egress}-depth bytes]
    [default 802.1p value]
    [default dscp value]
    [default classification {802.1p | tos | dscp}]
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

**Defaults**

- All ports are untrusted.
- By default, QoS ports do not preempt queues of lower priority.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **trusted** option to change the trust mode for the port.

**Examples**

```
-> qos port 1/3/1 trusted
-> qos port 1/4/2 no trusted
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **qos port trusted**  
  Configures whether the default mode for QoS ports is trusted or untrusted.

- **show qos port**  
  Displays information about QoS ports.

**MIB Objects**

- `alaQoSPortTable`
  - `alaQoSPortSlot`
  - `alaQoSPortPort`
  - `alaQoSPortTrusted`
  - `alaQoSPortMaximumBandwidth`
  - `alaQoSPortMaximumBandwidthStatus`
  - `alaQoSPortMaximumIngBandwidth`
  - `alaQoSPortMaximumIngBandwidthStatus`
  - `alaQoSPortMaximumDefaultDepth`
  - `alaQoSPortMaximumDefaultDepthStatus`
  - `alaQoSPortDefault8021p`
  - `alaQoSPortDefaultDSCP`
  - `alaQoSPortDefaultClassification`
qos port trusted

Configures whether an individual port is trusted or untrusted. Trusted ports can accept the 802.1p and ToS/DSCP values in incoming packets; untrusted ports will set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured.

```plaintext
qos port chassis/slot/port[-port2] trusted
qos port chassis/slot/port no trusted
```

### Syntax Definitions

chassis
The chassis identifier.

slot/port[-port2]
A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

### Defaults

By default, all ports are untrusted.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `qos trust-ports` command to set the default trust mode for all QoS ports. The `qos port trusted` command may be used to override the default.
- The setting applies only to ports with incoming traffic.
- Use the `qos port default 802.1p` or `qos port default dscp` commands to specify that a value other than zero should be applied to the incoming packets. Note that this value is overridden if a policy exists that specifies a different 802.1p or ToS/DSCP value for such packets.

### Examples

```
-> qos port 1/3/1 trusted
-> qos port 1/4/2 no trusted
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.
- **qos port**
  Configures a physical port for QoS.
- **qos trust-ports**
  Configures the global trust mode for QoS ports.
- **show qos port**
  Displays information about QoS ports.

**MIB Objects**

- **alaQoSPortTable**
  - **alaQoSPortTrusted**
**qos port maximum egress-bandwidth**

Configures the maximum rate at which the traffic is sent on the specified QoS port.

```
qos port chassis/slot/port[-port2] maximum egress-bandwidth bps [k | m | g | t]
qos port chassis/slot/port[-port2] no maximum egress-bandwidth
```

**Syntax Definitions**

- `chassis` - The chassis identifier.
- `slot/port[-port2]` - A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
- `bps[k | m | g | t]` - The maximum amount of bandwidth, in bits-per-second, for all traffic that egresses on the port. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k, 5m, 1g, 1t).

**Defaults**

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>k</td>
<td>m</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a configured maximum egress bandwidth value from a port.
- If the maximum egress bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number 10 is specified, 10K is the maximum bandwidth value used. However, if 10G is specified, the maximum bandwidth value applied is 10 gbps.
- The maximum egress bandwidth value cannot exceed the maximum bandwidth of the interface type associated with the port.
- Modifying the maximum egress bandwidth is most useful for low-bandwidth links.
Examples

- `qos port 3/1 maximum egress-bandwidth 10`
- `qos port 4/1-8 maximum egress-bandwidth 10g`
- `qos port 3/1 no maximum egress-bandwidth`
- `qos port 4/1-8 no maximum egress-bandwidth`

Release History

Release 7.1.1; command was introduced.

Related Commands

- `qos port maximum ingress-bandwidth`  Configures the rate at which traffic is received on a QoS port.
- `qos apply`  Applies configured QoS and policy settings to the current configuration.
- `qos port`  Configures a physical port for QoS.
- `show qos port`  Displays information about QoS ports.

MIB Objects

- `alaQoSPortTable`
  - `alaQoSPortSlot`
  - `alaQoSPortPort`
  - `alaQoSPortMaximumBandwidth`
  - `alaQoSPortMaximumBandwidthStatus`
**qos port maximum ingress-bandwidth**

Configures the maximum rate at which traffic is received on a QoS port.

```
qos port chassis/slot/port[-port2] maximum ingress-bandwidth bps [k | m | g | t]
qos port chassis/slot/port[-port2] no maximum ingress-bandwidth
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
- `bps[k | m | g | t]` The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k, 5m, 1g, 1t).

**Defaults**

By default, the maximum bandwidth is the maximum allowed for the interface type on which the port resides.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>k</td>
<td>m</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a configured maximum ingress bandwidth value from a port.

- If the maximum ingress bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number 10 is specified, 10K is the maximum bandwidth value used. However, if 10G is specified, the maximum bandwidth value applied is 10 gbps.

- The maximum ingress bandwidth value cannot exceed the maximum bandwidth of the interface type associated with the port.

- Modifying the maximum ingress bandwidth is most useful for low-bandwidth links.
Examples

-> qos port 3/1 maximum ingress-bandwidth 10
-> qos port 4/1-8 maximum ingress-bandwidth 10g
-> qos port 3/1 no maximum ingress-bandwidth
-> qos port 4/1-8 no maximum ingress-bandwidth

Release History

Release 7.1.1; command introduced.

Related Commands

qos port maximum egress-bandwidth  
Configures the rate at which traffic is sent on a QoS port.

qos apply
Applies configured QoS and policy settings to the current configuration.

qos port
Configures a physical port for QoS.

show qos port
Displays information about QoS ports.

MIB Objects

alaQoSPortTable
alaQoSPortSlot
alaQoSPortPort
alaQoSPortMaximumIngBandwidth
alaQoSPortMaximumIngBandwidthStatus
**qos port maximum depth**

Configures the maximum queue depth or bucket size assigned to this action, in bytes, used for traffic metering. The queue depth or bucket size determines the amount of buffer allocated to each queue. When the queue depth or bucket size is reached, the switch starts dropping packets.

```
qos port chassis/slot/port[-port2] maximum {ingress | egress}-depth bytes [k | m | g | t]
qos port chassis/slot/port[-port2] no maximum {ingress | egress}-depth
```

**Syntax Definitions**

- **chassis**
  The chassis identifier.

- **slot/port[-port2]**
  A physical slot and port number. Use a hyphen to specify a range of ports.

- **bytes[k | m | g | t]**
  The maximum bucket size, in bytes. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k, 5m).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>k</td>
<td>m</td>
</tr>
<tr>
<td>bytes</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This QoS port parameter is configured in conjunction with the maximum bandwidth parameters. When the bucket size is reached, the switch starts to drop packets.

- Use the `no` form of the command to remove the maximum depth setting from a port.

- If the maximum depth value is specified as an integer, without an abbreviated unit designation, the value is applied in Kbytes by default. For example, if the number 10 is specified, 10K is the maximum depth value used. However, if 1M is specified, the maximum depth value applied is 1 Mbyte.

- Modifying the maximum depth is most useful for low-bandwidth links.
**Examples**

-> qos port 3/1 maximum ingress-depth 10
-> qos port 4/1-8 maximum egress-depth 1m
-> qos port 3/1 no maximum ingress-depth
-> qos port 4/1-8 no maximum egress-depth

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **qos apply**
  - Applies configured QoS and policy settings to the current configuration.

- **qos port**
  - Configures a physical port for QoS.

- **show qos port**
  - Displays information about QoS ports.

**MIB Objects**

- alaQoSPortTable
  - alaQoSPortSlot
  - alaQoSPortPort
  - alaQoSPortMaximumDefaultDepth
  - alaQoSPortMaximumDefaultDepthStatus
  - alaQoSPortMaximumIngressDepth
  - alaQoSPortMaximumIngressDepthStatus
**qos port default 802.1p**

Configures the 802.1p value to be inserted in flows ingressing on an untrusted port.

**qos port chassis/slot/port[-port2] default 802.1p value**

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
- **value**: The priority value to be set. Values range from 0 (lowest priority) to 7 (highest priority).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- By default untrusted ports will set the 802.1p bit to zero on incoming flows. Use this command to specify that a different 802.1p value should be applied to the flow.
- The default 802.1p value is not used if there is a matching QoS policy rule that sets the priority.
- Note that the 802.1p bit for tagged packets received on untrusted ports is set with the default 802.1p value, which is configured using the **qos port default 802.1p** command. If the packet is untagged, however, then the DSCP bit is set with the default DSCP value, which is configured using the **qos port default dscp** command.

---

**Examples**

- `-> qos port 3/1 default 802.1p 5`
- `-> qos port 4/1-8 default 802.1p 7`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

qos apply
Applies configured QoS and policy settings to the current configuration.

qos port
Configures a physical port for QoS.

show qos port
Displays information about QoS ports.

MIB Objects
alaQoSPortTable
alaQoSPortDefault8021p
**qos port default dscp**

Configures the ToS/DSCP value to be inserted in flows ingressing on an untrusted port.

```command
text
```

**Syntax Definitions**

- `chassis` - The chassis identifier.
- `slot/port[-port2]` - A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
- `value` - The ToS/DSCP value. The range is 0–63.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>chassis</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The value configured by this command sets the upper byte (precedence) and therefore configures the ToS/DSCP value for the port.
- The default DSCP value is not used if there is a matching QoS policy rule that sets the priority.
- Note that on the 802.1p bit for tagged packets received on untrusted ports is set with the default 802.1p value, which is configured using the `qos port default 802.1p` command. If the packet is untagged, however, then the DSCP bit is set with the default DSCP value, which is configured using the `qos port default dscp` command.

**Examples**

```
-> qos port 3/1 default dscp 63
-> qos port 4/1-8 default dscp 33
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **qos port**: Configures a physical port for QoS.
- **show qos port**: Displays information about QoS ports.

MIB Objects

- **alaQoSPortTable**
  - **alaQoSPortDefaultDSCP**
**qos port default classification**

Specifies the default egress priority value to use for IP traffic ingressing on trusted ports.

```
qos port chassis/slot/port[-port2] default classification {tos | 802.1p | dscp}
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.
- **slot/port[-port2]**
  - A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).
- **tos**
  - Specifies that the ToS value of the flow will be used to prioritize flows coming in on the port.
- **802.1p**
  - Specifies that the 802.1p value of the flow will be used to prioritize flows coming in on the port.
- **dscp**
  - Specifies that the DSCP value of the flow will be used to prioritize flows coming in on the port.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>tos</td>
<td>802.1p</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The egress priority assigned to an IP packet received on a trusted port is based on the DSCP value of the packet unless 802.1p is specified using this command.

- The default classification priority is not used if there is a matching QoS policy rule that sets the egress priority value.

- This command does not affect Layer 2 traffic, which is always classified with 802.1p.

- In some network situations, some IP traffic may be dropped before any QoS rules can take effect for the traffic.
Examples

- `qos port 8/24 default classification dscp`
- `qos port 4/1-8 default classification dscp`
- `qos port 7/1 default classification 802.1p`
- `qos port 5/1-8 default classification 802.1p`

Release History

Release 7.1.1; command was introduced.

Related Commands

- `qos apply` Applies configured QoS and policy settings to the current configuration.
- `qos port` Configures a physical port for QoS.
- `show qos port` Displays information about QoS ports.

MIB Objects

- `alaQoSPortTable` `alaQoSPortDefaultClassification`
**qos port dei**

Configures the Drop Eligible Indicator (DEI) bit mapping and marking setting for the specified QoS port. The DEI setting applies to packets marked yellow (non-conforming) as the result of Tri-Color Marking (TCM) or other rate limiting mechanisms.

```bash
qos port chassis/slot/port dei {ingress | egress}
qos port chassis/slot/port no dei {ingress | egress}
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (1/5).
- `ingress` Maps the DEI/CFI bit to yellow (non-conforming) if this bit is set for ingress traffic. **DEI mapping is not supported on the OmniSwitch 6465.**
- `egress` Marks the DEI/CFI bit for egress packets if the packets were marked yellow as a result of the rate limiting process.

**Defaults**

By default, no DEI/CFI bit mapping or marking is done.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the DEI bit mapping (ingress) or marking (egress) configuration for the specified port.
- Use the `qos dei` command to set the global DEI bit mapping and marking configuration for all QoS switch ports. Note that the port-level setting takes precedence over the global DEI setting.
- Packets marked yellow by rate limiting are still transmitted when there is no congestion on the egress port queues. Setting the DEI bit for yellow egress packets (`qos port dei egress`) ensures that an upstream switch is made aware that the packet was marked yellow.
- When a switch receives a yellow packet with the DEI bit set and ingress DEI bit mapping is enabled (`qos port dei ingress`), the packet is mapped to an internal drop precedence or yellow color marking for the switch.
DEI bit mapping is not supported on the OmniSwitch 6465. As a result, packets are processed as follows on that switch:

- When packets are received on a trusted port, the DEI bit is retained only if the packets were not subject to a meter. If the port is untrusted, however, the DEI bit is always reset.
- When a meter is set and DEI egress is configured on a trusted port, the DEI bit is reset to 0 for green packets. Yellow–red packets egress with the DEI bit set to 1.

When the port is untrusted, DEI ingress is not supported on the OmniSwitch 6560 and OmniSwitch 6570M.

Examples

- `qos port 1/10 dei ingress`
- `qos port 1/20 dei egress`
- `qos port 1/10 no dei ingress`
- `qos port 1/20 no dei egress`

Release History

Release 7.2.1; command was introduced.

Related Commands

- `qos port` Configures a physical port for QoS.
- `qos dei` Configures the global Drop Eligible Indicator (DEI) bit mapping and marking setting for all QoS ports.
- `policy action cir` Configures a Tri-Color Marking policy action.
- `show qos config` Displays global information about the QoS configuration.
- `show qos port` Displays information about QoS ports.

MIB Objects

- `alaQoSPortTable`
- `alaQoSPortDEIMapping`
- `alaQoSPortDEIMarking`
### qos qsp import

Imports a predefined QSet profile (QSP) to a new or previous custom profile.

```
qos qsp {qsp_id | qsp_name} import qsp {import_qsp_id | import_qsp_name}
no qos qsp {qsp_id | qsp_name}
```

#### Syntax Definitions

- **qsp_id**: A QSet custom profile ID. The valid custom profile ID range is 6–16.
- **qsp_name**: The QSet profile name.
- **import_qsp_id**: The ID of the QSet profile to import.
- **import_qsp_name**: The name of the QSet profile to import.

#### Defaults

N/A

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X72</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- The new QSet profile must be unique and not contain the same name and ID of an existing QSet profile.
- Use the `no` form of the command to remove an existing custom QSet profile from the switch configuration.
- On the OmniSwitch 6360, OmniSwitch 6860N, OmniSwitch 6900-V72/C32, and OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8, the custom profile ID range is 3–8.
- On the OmniSwitch 6465, the custom profile ID range is 6–8.
- The following table lists which predefined QSPs can be used to import as a base for custom profiles:
The predefined QSet profiles cannot be removed from the switch configuration.

A custom profile can be assigned to any port or link aggregate, but not to a VFL link.

A custom profile attached to a port cannot be removed from the switch configuration. In this case, the profile must be disassociated from the port before being removed.

**Examples**

- `-> qos qsp 12 import qsp 1`
- `-> qos qsp qsp-16 import qsp 5`
- `-> no qsp 12`

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

- **qos qsi qsp**
  Configures the QSet profile association for the QSet instance.

- **show qos qsp**
  Displays the QSet profile attributes.

**MIB Objects**

- `alaVfcQsetProfileTable`  
- `alaVfcQSPId`
- `alaVfcQSPName`
- `alaVfcQSPTemplateId`
- `alaVfcQSPTemplateName`
- `alaVfcQSPRowStatus`
qos qsp qp

Modifies the Committed Information Rate (CIR), Peak Information Rate (PIR), scheduler, WFQ weight attributes for an individual queue profile (QP) associated with a custom QSet profile (QSP).

```
qos qsp {qsp_id | qsp_name} qp qp_id {cir % | pir % | weight weight | scheduler {sp | wrr | wrr2}}
```

### Syntax Definitions

- **qsp_id**: A QSet custom profile ID. The valid custom profile ID range is 6–16.
- **qsp_name**: The QSet custom profile name.
- **qp_id**: The queue profile number in the QSet custom profile.
- **cir %**: The Committed Information Rate to apply to queue traffic. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, OmniSwitch 6570M and OmniSwitch 9900.
- **pir %**: The Peak Information Rate limit to apply to queue traffic.
- **weight**: The queue weight that is used to determine the amount of shared bandwidth allocated for queue traffic. The valid range is 1–100.
- **sp**: Selects the Strict Priority (SP) scheduler. This parameter is supported only on the OmniSwitch 6360 and OmniSwitch 6465.
- **wrr**: Selects the Weighted Round Robin scheduler (WRR). This parameter is supported only on the OmniSwitch 6360 and OmniSwitch 6465.
- **wrr2**: This parameter is not supported.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The queue weight value is only used when WRR is the scheduler for the queue.
- The **cir**, **pir**, and **weight** attributes are only configurable for individual queues that are associated with a custom QSet profile. Changing the scheduler attribute is not supported.
- Changing the scheduler attribute is supported only on the OmniSwitch 6360 and OmniSwitch 6465.
• When a custom profile is modified, the changes are applied to all ports that are associated with that custom profile. To apply specific changes to a single port (QSet instance), import a predefined profile into a new custom profile, make the necessary changes, then apply the new custom profile to the port.

• Custom QSet profile supports a combination of SP and WRR schedulers configuration in the same QSet profile. For example, a custom QSet profile can have SP applied to one queue, and WRR scheduler to another queue.

**Examples**

```
-> qos qsp 6 qp 1 weight 2 pir 100
-> qos qsp 6 qp 2 weight 1 pir 100
-> qos qsp 6 qp 3 weight 3 pir 100
-> qos qsp 6 qp 4 weight 4 pir 100
-> qos qsp 6 qp 5 weight 2 pir 100
-> qos qsp 6 qp 6 cir 10 pir 50
-> qos qsp 6 qp 7 weight 2 pir 100
-> qos qsp 6 qp 8 scheduler sp
ERROR: scheduler change is not supported.
```

The following example shows the custom QSet profile configured with a combination of strict priority and WRR schedulers applied to different queues of the same QSet profile.

```
-> qos qsp "ale-qsp-5" import qsp "qsp-5"
-> qos qsp "ale-qsp-5" qp 1 weight 15
-> qos qsp "ale-qsp-5" qp 3 pir 20 scheduler sp
-> qos qsp "ale-qsp-5" qp 8 weight 4
```

**Release History**

Release 8.3.1.R02; command was introduced.
Release 8.7R1; scheduler parameter deprecated.
Release 8.8R2; scheduler parameter supported on OmniSwitch 6360 and OmniSwitch 6465.

**Related Commands**

- `qos qsp import` Creates a custom QSet profile.
- `show qos qsp` Displays the QSet profile attributes.

**MIB Objects**

```
alaVfcQProfileTable
alaVfcQProfileId
alaVfcQProfileName
alaVfcQProfile
alaVfcQPCIRBandwidthLimitType
alaVfcQPCIRBandwidthLimitValue
alaVfcQPPIRBandwidthLimitType
alaVfcQPPIRBandwidthLimitValue
alaVfcQPWFqWeight
alaVfcQPWFqMode
```
**qos qsi qsp**

Configures the QSet profile (QSP) association for the specified QSet instance (QSI). A QSI is a set of eight queues that is automatically associated with each port, link aggregate, and virtual fabric link (VFL).

```bash
qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[agg_id2] | vf-link vfl_id} qsp {qsp_id | qsp_name}
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).

- **agg_id[agg_id2]**
  - The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).

- **vfl_id**
  - The VFL link ID (1/0). *This parameter option is supported only on the OmniSwitch 6860, OmniSwitch 6860N, and OmniSwitch 6865.*

- **qsp_id**
  - An existing QSet profile (QSP) ID number to assign to this instance. Refer to the table in the “Usage Guidelines” section of this command page for a list of the supported QSP IDs.

- **qsp_name**
  - An existing QSet profile name (for example, qsp-1) to assign to this instance.

### Defaults

By default, QSP 1 is assigned to each QSet instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- There is only one QSI for each port, link aggregate, and VFL and only one QSP associated with each QSI.

- A QSI hierarchy exists consisting of parent/child relationships. For example, all member ports of a link aggregate will import the QSI/QSP settings of the parent link aggregate. When a member port moves out of the link aggregate, the QSI/QSP settings for that port are reset to the default settings.

- The number of children supported for a LAG ID is 8.

- Use the following table to determine which QSP IDs a specific switch platform supports and whether configuring a custom QSP is supported on that platform:
On an OmniSwitch 6860, OmniSwitch 6860N, or OmniSwitch 6865, changing the QSP assignment for one VFL instance automatically changes the QSP assignment for all of the other VFL instances to the same QSP. For example, if QSP 2 is assigned to VFL 1/0, then the QSP assignment for VFL 2/0 is also changed to QSP 2. It is not necessary to configure the QSP assignment separately for each VFL on the switch.

**Examples**

-> qos qsi port 1/1/2 qsp 2  
-> qos qsi port 1/2/1-10 qsp 3  
-> qos qsi slot 3 qsp 4  
-> qos qsi linkagg 10 qsp 2

The following command examples show that when the QSP assignment for VFL 1 is changed to QSP 2, the QSP for VFL 2 is automatically changed as well:

-> qos qsi vf-link 1/0 qsp 2  
WARNING: configuration change applied to all VFLs in the system

-> show qos qsi vf-link 1/0 summary
Legends: * indicates port is misconfigured.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Port</th>
<th>Name</th>
<th>Mode</th>
<th>Parent</th>
</tr>
</thead>
<tbody>
<tr>
<td>vfl-1/0</td>
<td>2</td>
<td>qsp-2</td>
<td>NDCB</td>
<td>vfl-1/0</td>
</tr>
</tbody>
</table>

-> show qos qsi vf-link 2/0 summary
Legends: * indicates port is misconfigured.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Port</th>
<th>Name</th>
<th>Mode</th>
<th>Parent</th>
</tr>
</thead>
<tbody>
<tr>
<td>vfl-2/0</td>
<td>2</td>
<td>qsp-2</td>
<td>NDCB</td>
<td>vfl-2/0</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.2.1.R02; command introduced.
Release 8.3.1; vf-link parameter added.

**Related Commands**

- **qos qsp import**
  Imports a predefined QSet profile (QSP) to a new or previous custom profile.

- **qos qsi stats**
  Configures statistics collection for the QSet instance.

- **show qos qsi**
  Displays the QSet instance configuration.

- **show qos qsp**
  Displays the QSet profile attributes.

**MIB Objects**

- alcatelIND1VfcMIB
- alaVfcQsetInstanceTable
  - alaVfcQsetId
  - alaVfcQsetQSPId
  - alaVfcQsetQSPName
**qos qsp system-default**

Changes the default QSet profile (QSP) that is assigned to each port, link aggregate ID, and virtual fabric link (VFL).

```
qos qsp system-default {qsp_id | qsp_name}
```

### Syntax Definitions

- **qsp_id**
  - An existing QSet profile (QSP) ID number to use as the default QSP.
  - The valid range is 1–4.

- **qsp_name**
  - An existing QSet profile name (qsp-1, qsp-2, qsp-3, qsp-4) to use as the default QSP.

### Defaults

By default, QSP 1 is assigned to each QSet instance.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When this command is used, the specified QSP is assigned to all ports, link aggregates, and VFLs on the switch.

- Changing the system default profile is only allowed when the switch is running in the non-Data Center Bridging (NDCB) mode. This mode is active by default when there is no OmniSwitch Data Center software license installed on the switch.

- A QSP assigned through the `qos qsi qsp` command overrides the system default QSP assignment. For example, if the system default QSP is set to 1 and the `qos qsi qsp` command is used to change the QSP to 2 on port 1/1/20, the QSP 2 settings are applied to port 1/1/20.

### Examples

```
-> qos qsp system-default 2
-> qos qsp system-default qsp-4
```

### Release History

Release 8.3.1; command introduced.
Related Commands

- **qos qsi qsp**  Configures the QSet profile association for the QSet instance.
- **show qos qsp system-default**  Displays the name and ID of the default QSP for the switch.

MIB Objects

- **alcatelIND1VfcMIB**
  - **alaVfcSystemDefaultQsetQSPName**
  - **alaVfcSystemDefaultQsetQSPId**
**qos qsi stats**

Configures the administrative status and interval for statistics collection for the specified QSet instance (QSI). A QSI is a set of eight queues that is automatically associated with each port and link aggregate (LAG) ID.

```
qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} stats {admin-state {enable | disable} | interval interval_time}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).
- **agg_id[-agg_id2]**: The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).
- **enable**: Enables statistics collection for the instance.
- **disable**: Disables statistics collection for the instance.
- **interval_time**: The time interval for statistics gathering. The valid range is 10–300 seconds.

### Defaults

By default, statistics collection is disabled and the time interval is set to 10 seconds.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- There is only one QSI per port or LAG ID and only one QSet profile (QSP) or DCB profile (DCP) associated with the QSI.
- Changing the statistics collection status for a QSI only changes the status for the port or link aggregate to which the QSI is associated.

### Examples

- `-> qos qsi port 1/2 stats admin-state enable`
- `-> qos qsi port 1/2 stats interval 30`
- `-> qos qsi port 2/1-10 stats admin-state enable`
- `-> qos qsi linkagg 10 stats admin-state enable interval 120`
QoS Commands

Release History

Release 7.2.1.R02; command introduced.

Related Commands

qos qsi qsp
Configures the QSet profile association for the QSet instance.

show qos qsi
Displays the QSet instance configuration.

show qos qsi stats
Displays statistics for one or more QSet instances.

MIB Objects

alcatelIND1VfcMIB
alaVfcQsetInstanceTable
  alaVfcQsetQSPId
  alaVfcQsetQSPName
  alaVfcQsetStatsAdmin
  alaVfcQsetStatsInterval
**show qos port**

Displays information about all QoS ports or a particular port.

`show qos port [chassis/slot/port]`

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2/ X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Information for all ports is displayed unless a particular port is specified.
- Use the `qos port` command to configure port parameters.
- For ports that are trusted (Yes displays in the Trust field), the Trust field includes one of the following characters:

<table>
<thead>
<tr>
<th>character</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Indicates that the port is manually configured as trusted through the <code>qos port trusted</code> command; the port setting takes precedence over the global trust setting configured through the <code>qos trust-ports</code> command.</td>
</tr>
<tr>
<td>*</td>
<td>Indicates that the port is automatically trusted regardless of the global setting set through the <code>qos trust-ports</code> command. (Applies to mobile ports and ports configured for 802.1Q.)</td>
</tr>
</tbody>
</table>

- Dash (`-`) in the Bandwidth signifies the ingress/egress default value, which is equal to the port physical bandwidth. This means, the maximum ingress/egress bandwidth is not explicitly configured.
### Examples

```plaintext
-> show qos port

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Active</th>
<th>Trust</th>
<th>Default P</th>
<th>Default DSCP</th>
<th>Default Classification</th>
<th>Physical Bandwidth</th>
<th>Ingress Bandwidth</th>
<th>Egress Bandwidth</th>
<th>DEI Map/Mark</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Yes</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>1.00G</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet-1G</td>
</tr>
<tr>
<td>1/1/3</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/4</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/5</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/6</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/7</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/8</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/9</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/10</td>
<td>No</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/11</td>
<td>No <em>Yes</em></td>
<td>No</td>
<td>0/0</td>
<td>*802.1P</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
<tr>
<td>1/1/12</td>
<td>No <em>Yes</em></td>
<td>No</td>
<td>0/0</td>
<td>*802.1P</td>
<td>0K</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet</td>
</tr>
</tbody>
</table>

-> show qos port 1/2

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Active</th>
<th>Trust</th>
<th>Default P</th>
<th>Default DSCP</th>
<th>Default Classification</th>
<th>Physical Bandwidth</th>
<th>Ingress Bandwidth</th>
<th>Egress Bandwidth</th>
<th>DEI Map/Mark</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>Yes</td>
<td>No</td>
<td>0/0</td>
<td>DSCP</td>
<td>1.00G</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>No / No</td>
<td>ethernet-1G</td>
</tr>
</tbody>
</table>
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot/Port</td>
<td>The slot and physical port number.</td>
</tr>
<tr>
<td>Active</td>
<td>Whether or not the port is sending/receiving QoS traffic.</td>
</tr>
<tr>
<td>Trust</td>
<td>Whether the port is trusted or not trusted. Configured through the <code>qos port trusted</code> command.</td>
</tr>
<tr>
<td>Default P</td>
<td>The default 802.1p setting for the port. Configured through the <code>qos port default 802.1p</code> command.</td>
</tr>
<tr>
<td>Default DSCP</td>
<td>The default ToS/DSCP setting for the port. Configured through the <code>qos port default dscp</code> command.</td>
</tr>
<tr>
<td>Default Classification</td>
<td>The default classification setting for the port (802.1p, ToS, or DSCP). Configured through the <code>qos port default classification</code> command.</td>
</tr>
<tr>
<td>Physical Bandwidth</td>
<td>The amount of physical bandwidth available on the port.</td>
</tr>
<tr>
<td>Ingress Bandwidth</td>
<td>The amount of ingress bandwidth configured for the port. Configured through the <code>qos port maximum ingress-bandwidth</code> command.</td>
</tr>
<tr>
<td>Egress Bandwidth</td>
<td>The amount of egress bandwidth configured for the port. Configured through the <code>qos port maximum egress-bandwidth</code> command.</td>
</tr>
<tr>
<td>DEI Map/Mark</td>
<td>The Drop Eligible Indicator (DEI) bit mapping and marking setting for the port. Configured through the <code>qos port dei</code> command.</td>
</tr>
<tr>
<td>Type</td>
<td>The interface type, <code>ethernet</code> or <code>wan</code>.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command was introduced.
**QoS Commands**

- `show qos port` Configures a physical port for QoS.

**Related Commands**

- `qos port` Configures a physical port for QoS.

**MIB Objects**

- alcatelIND1VfcMIB
- alaQoSPortTable
  - alaQoSPortSlot
  - alaQoSPortPort
  - alaQoSPortInterfaceType
  - alaQoSPortTrusted
  - alaQoSPortDefault8021p
  - alaQoSPortDefaultDSCP
  - alaQoSPortMaximumDefaultDepth
  - alaQoSPortMaximumDefaultDepthStatus
  - alaQoSPortReset
  - alaQoSPortPhysicalBandwidth
  - alaQoSPortRowStatus
  - alaQoSPortDefaultClassification
  - alaQoSPortMaximumBandwidth
  - alaQoSPortMaximumBandwidthStatus
  - alaQoSPortMaximumIngressBandwidth
  - alaQoSPortMaximumIngressBandwidthStatus
  - alaQoSPortMaximumIngressDepth
  - alaQoSPortMaximumIngressDepthStatus
  - alaQoSPortDEIMarking
  - alaQoSPortDEIMapping
show qos slice

Displays rule availability and usage information for QoS slices of QoS slots. A slice is a logical section of hardware and corresponds to particular ports on the interface.

show qos slice [slot/slice]

Syntax Definitions

slot/slice The slot number and slice for which you want to view information. The number of slices per module varies depending on the type of module.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Information for all slots/slices is displayed unless a particular slot/slice is requested.
- This command is useful for monitoring switch resources required for policy rules.
- On the following switch platforms, use the show tcam utilization command instead of the show qos slice command:
  - OmniSwitch 6360
  - OmniSwitch 6465
  - OmniSwitch 6560
  - OmniSwitch 6570M
  - OmniSwitch 6860N
  - OmniSwitch 6900-V72/C32
  - OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8
  - OmniSwitch 9900

Examples

-> show qos slice

<table>
<thead>
<tr>
<th>Slot/Unit</th>
<th>Type</th>
<th>Total/Free</th>
<th>Rules</th>
<th>Counters</th>
<th>Meters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/(0)</td>
<td>IFP</td>
<td>24/24</td>
<td>0</td>
<td>256/252</td>
<td>256/256</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>256/255</td>
<td>256/255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>256/256</td>
<td>256/256</td>
</tr>
</tbody>
</table>
QoS Commands

show qos slice

<table>
<thead>
<tr>
<th>Slot/Unit</th>
<th>Type</th>
<th>Ranges Total</th>
<th>Ranges Free</th>
<th>CAM</th>
<th>Rules Total</th>
<th>Rules Free</th>
<th>Counters Total</th>
<th>Counter Free</th>
<th>Meters Total</th>
<th>Meters Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/(0)</td>
<td>EFP</td>
<td>0/0</td>
<td>0/0</td>
<td>0/0</td>
<td>256/256</td>
<td>256/256</td>
<td>256/255</td>
<td>256/254</td>
<td>256/255</td>
<td>256/256</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td>256/256</td>
<td>256/256</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>256/255</td>
<td>256/254</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td>256/255</td>
<td>256/254</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

output definitions

- **Slot/Unit**: The slot and slice number.
- **Type**: The type of slice.
- **Ranges Total**: The total number of TCP/UDP port ranges supported per slot/slice.
- **Ranges Free**: The number of TCP/UDP port ranges that are still available for use.
- **CAM**: The CAM number.
- **Rules Total**: The total number of rules supported per CAM.
- **Rules Free**: The number of rules that are still available for use. On startup, the switch uses 27 rules.
- **Counters Total**: The total number of counters supported per CAM.
- **Counter Free**: The number of counters that are still available for use.
- **Meters Total**: The total number of meters supported per CAM.
- **Meters Free**: The number of meters that are still available for use.

Release History

Release 7.1.1; command was introduced.

Related Commands

- **policy rule**: Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

N/A
show qos log

Displays the log of QoS events.

show qos log

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to display the current QoS log. To clear the log, use the `clear qos log` command.

Examples

-> show qos log  
**QOS Log**
Insert rule 0
Rule index at 0
Insert rule 1
Rule index at 1
Insert rule 2
Rule index at 2
Enable rule r1 (1) 1,1
Enable rule r2 (0) 1,1
Enable rule yubal (2) 1,1
Verify rule r1(1)
Enable rule r1 (1) 1,1
Really enable r1
Update condition c1 for rule 1 (1)
Verify rule r2(1)
Enable rule r2 (0) 1,1
Really enable r2
Update condition c2 for rule 0 (1)
Verify rule yubal(1)
Enable rule yubal (2) 1,1
Really enable yubal
Update condition yubamac for rule 2 (1)
QoS Manager started TUE MAR 10 13:46:50 2002

Match rule 2 to 1
Match rule 2 to 2
Match rule 2 to 3

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

*clear qos log*  
Clears messages in the current QoS log.

*qos log lines*  
Configures the number of lines in the QoS log.

**MIB Objects**

N/A
**show qos config**

Displays global information about the QoS configuration.

**show qos config**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to view the current global configuration for QoS. Use the **show qos statistics** command to view statistics about the QoS software in the switch.

**Examples**

```plaintext
-> show qos config
QoS Configuration
Admin = enable,
Switch Group = expanded,
Trust ports = no,
Phones = trusted,
Log lines = 10240,
Log level = 5,
Log console = no,
Forward log = no,
Stats interval = 60,
User-port filter = spoof,
User-port shutdown = none,
Debug = info,
DEI Mapping = Disabled,
DEI Marking = Disabled,
Pending changes = none
```
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Whether or not QoS is enabled or disabled. Configured through the <code>qos</code> command.</td>
</tr>
<tr>
<td>Switch Group</td>
<td>Whether the expanded or compact method is used to populate the hardware routing table. Configured through the <code>qos switch-group</code> command.</td>
</tr>
<tr>
<td>Trust Ports</td>
<td>The default trusted mode for switch ports. Configured through the <code>qos trust-ports</code> command.</td>
</tr>
<tr>
<td>Phones</td>
<td>Whether or not IP Phone traffic is automatically trusted or assigned a priority value. Configured through the <code>qos phones</code> command.</td>
</tr>
<tr>
<td>Log lines</td>
<td>The number of lines included in the QoS log. Configured through the <code>qos log lines</code> command.</td>
</tr>
<tr>
<td>Log level</td>
<td>The level of log detail. Configured through the <code>qos log level</code> command.</td>
</tr>
<tr>
<td>Log console</td>
<td>Whether or not log messages are sent to the console. Configured through the <code>qos log console</code> command.</td>
</tr>
<tr>
<td>Forward log</td>
<td>Whether or not logged events are sent to the policy server software in the switch in real time. Configured through the <code>qos forward log</code> command.</td>
</tr>
<tr>
<td>Stats interval</td>
<td>How often the switch polls network interfaces for statistics about QoS events. Configured through the <code>qos stats interval</code> command.</td>
</tr>
<tr>
<td>User-port filter</td>
<td>The type of traffic that is filtered on ports that are members of the UserPorts group. Configured through the <code>qos user-port</code> command.</td>
</tr>
<tr>
<td>User-port shutdown</td>
<td>The type of traffic that will trigger an administrative shutdown of the port if the port is a member of the UserPorts group. Configured through the <code>qos user-port</code> command.</td>
</tr>
<tr>
<td>Debug</td>
<td>The type of information that will be displayed in the QoS log. A value of <code>info</code> indicates the default debugging type.</td>
</tr>
<tr>
<td>DEI Mapping</td>
<td>The status (enabled or disabled) of Drop Eligible Indicator (DEI) bit mapping for ingress traffic. Configured through the <code>qos dei</code> command.</td>
</tr>
<tr>
<td>DEI Marking</td>
<td>The status (enabled or disabled) of DEI bit marking for egress traffic. Configured through the <code>qos dei</code> command.</td>
</tr>
<tr>
<td>Pending changes</td>
<td>QoS changes not yet applied to the configuration.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
**Related Commands**

**qos**

Enables or disables QoS. This base command may be used with keyword options to configure QoS globally on the switch.

**show qos statistics**

Displays statistics about the QoS configuration.

**MIB Objects**

alaQoSConfigTable

- alaQoSConfigEnable
- alaQoSConfigSwitchGroup
- alaQoSConfigTrustPorts
- alaQoSConfigAutoPhones
- alaQoSConfigLogLines
- alaQoSConfigLogLevel
- alaQoSConfigLogConsole
- alaQoSConfigStatsInterval
- alaQoSConfigUserportFilter
- alaQoSConfigUserportShutdown
- alaQoSConfigDebug
- alaQoSConfigDEIMapping
- alaQoSConfigDEIMarking
show qos statistics

Displays statistics about the QoS configuration.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays statistics about the global QoS configuration. Use the `show qos config` command to display information about configurable global parameters.

**Examples**

```
-> show qos statistics
QoS stats

L2 Events : 0 0 0
L3 Inbound : 0 0 0
L3 Outbound : 0 0 0
IGMP Join : 0 0 0
Fragments : 0
Bad Fragments : 0
Unknown Fragments : 0
Sent NI messages : 0
Received NI messages : 85
Failed NI messages : 4
Max PTREE nodes : 0
Max PTREE depth : 0
Spoofed Events : 0
NonSpoofed Events : 0

Software resources

<table>
<thead>
<tr>
<th>Table</th>
<th>CLI</th>
<th>LDAP</th>
<th>Blt</th>
<th>Total</th>
<th>CLI</th>
<th>LDAP</th>
<th>Blt</th>
<th>Total</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>rules</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>8192</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th></th>
<th>Used</th>
<th>Free</th>
<th>Max</th>
<th>Used</th>
<th>Free</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCAM</td>
<td>0</td>
<td>1023</td>
<td>1024</td>
<td>0</td>
<td>32</td>
<td>32</td>
</tr>
</tbody>
</table>

**Actions**
- The number of Layer 2 or Layer 3 flows transmitted on the switch.

**Conditions**
- The number of Layer 2 or Layer 3 flows that match policies.

**Drops**
- The number of Layer 2 or Layer 3 flows that were dropped.

**L2**
- The number of Layer 2 events, matches, and drops.

**L3 Ingress**
- The number of Layer 3 ingress events, matches, and drops.

**L3 Egress**
- The number of Layer 3 egress events, matches, and drops.

**IGMP join**
- The number of multicast events, matches, and drops.

**Fragments**
- The number of fragments dropped.

**Bad Fragments**
- The number of fragments received with an offset of 1.

**Unknown Fragments**
- The number of out-of-order fragments received.

**Sent NI messages**
- The number of messages sent to network interfaces.

**Received NI messages**
- The number of messages received by network interfaces.

**Failed NI messages**
- The number of failed message attempts to network interfaces.

**Load balanced flows**
- The number of Server Load Balance flow entries.

**Reflexive flows**
- The number of reflexive flows.

**Reflexive correction**
- The number of reflexive flow corrections.

**Flow lookups**
- The number of flow table lookups.

**Flow hits**
- The number of flow table lookup hits.

**Max PTree nodes**
- The highest number of nodes in the classifier tree.

**Max Ptree depth**
- The length of the longest path in the classifier tree.

**Spoofed Events**
- The number of spoofed events.

**Nonspoofed Events**
- The number of non-spoofed events.

**DropServices**
- The number of TCP/UDP flows dropped.

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**qos stats reset**
Resets QoS statistic counters to zero.

**MIB Objects**

alaQoSStats
alaQoSStatsL2Events
alaQoSStatsL2matches
alaQoSStatsL2Drops
alaQoSStatsL3IngressEvents
alaQoSStatsL3IngressMatches
alaQoSStatsL3IngressDrops
alaQoSStatsL3EgressEvents
alaQoSStatsL3EgressMatches
alaQoSStatsL3EgressDrops
alaQoSStatsFragments
alaQoSStatsBadFragments
alaQoSStatsUnknownFragments
alaQoSStatsSpoofedEvents
alaQoSStatsNonspoofedEvents
**show qos qsi summary**

Displays a list of switch ports showing the QoS or DCB profile assigned to each port.

```
show qos qsi [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] summary
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (1/5-10).

- **agg_id[-agg_id2]**
  - A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

### Defaults

By default, a summary of all ports is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/X48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Enter a port or link aggregate ID with this command to display information for a specific port or link aggregate.

### Examples

```
-> show qos qsi summary
Legends: * indicates port is misconfigured.

<table>
<thead>
<tr>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>1/1/1</td>
</tr>
<tr>
<td>1/1/2</td>
</tr>
<tr>
<td>1/1/3</td>
</tr>
<tr>
<td>1/1/4</td>
</tr>
<tr>
<td>1/1/5</td>
</tr>
<tr>
<td>1/1/6</td>
</tr>
</tbody>
</table>

-> show qos qsi port 1/1-5 summary
Legends: * indicates port is misconfigured.

<table>
<thead>
<tr>
<th>Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>---------</td>
</tr>
</tbody>
</table>
```
### QoS Commands

show qos qsi summary

<table>
<thead>
<tr>
<th>Port</th>
<th>Profile</th>
<th>Name</th>
<th>Mode</th>
<th>Parent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>qsp-1</td>
<td>NDCB 1/1/1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/2</td>
<td>qsp-1</td>
<td>NDCB 1/1/2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/3</td>
<td>qsp-1</td>
<td>NDCB 1/1/3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/4</td>
<td>qsp-1</td>
<td>NDCB 1/1/4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/5</td>
<td>qsp-7</td>
<td>NDCB 1/1/5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

- **Port**: Configured DCB ports.
- **Profile #**: Identifies the DCB profile assigned to the port.
- **Profile Name**: Name of the DCB profile assigned to the port.
- **Mode**: Indicates if the port is DCB or NDCB.
- **Parent**: Lists the parent of the port.

### Release History

Release 7.3.1; command was introduced.

### Related Commands

- **show qos qsi dcb dcbx**: Displays the configured ports in the system and the related DCBX information.
- **qos qsi qsp dcb**: Assigns a DCB profile to a port or link aggregate.

### MIB Objects

- `alaVfcQsetInstanceTable`
  - `alaVfcQsetId`
  - `alaVfcQsetQSPId`
  - `alaVfcQsetQSPName`
  - `alaDcbxPortInstanceTable`
  - `alaVfcQsapParent`
**show qos qsp**

Displays the QSet profile (QSP) configuration for the switch.

```
show qos qsp [qsId | qsName] [brief | detail [port chassis/slot/port[-port2]] | linkagg agg_id[-agg_id2]]
```

---

**Syntax Definitions**

- **qsId**
  - A QSet profile (QSP) ID number. Refer to the table in the “Usage Guidelines” section for a list of the supported QSP IDs.

- **qsName**
  - The name of a QSP profile.

- **brief**
  - Displays a summary of the QSP configuration.

- **detail**
  - Displays QSP configuration details for a specific profile, port, slot, or link aggregate.

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - A physical slot and port number. Use a hyphen to specify a range of ports (1/5-10).

- **agg_id[-agg_id2]**
  - The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

---

**Defaults**

By default, displays the configuration for all of the QSet profiles.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `qsId` or the `qsName` parameter to display information for a specific profile.

- Use the `detail` parameter in combination with the `port slot/port` and `linkagg agg_id` parameters to display profile information associated with specific ports or link aggregates.

- Configuring a QSP assignment for a virtual fabric link (VFL) is supported only on the OmniSwitch 6860, OmniSwitch 6860N, and OmniSwitch 6865.

- The following QSPs are supported on the specified switch platforms:
QoS Commands

QoS Commands

show qos qsp

QSP2 has all WRR schedulers.

Examples

-> show qos qsp 1
QSP 1 (qsp-1)
  #Ports: 107, #Queues: 8, BW (%): 100,
  WRP: 1, Name: wrp-1
  Scheduler: Qspec, Type: Sta,
  Template: 1, Name: qsp-1
  QP 1
    Qtype: SP7,
    WRP: 1, Name: wrp-1
    CIR (%): 0, PIR (%): 100,
    WFQ-Mode: WERR, WFQ-Weight: 1
  QP 2
    Qtype: SP6,
    WRP: 1, Name: wrp-1
    CIR (%): 0, PIR (%): 100,
    WFQ-Mode: WERR, WFQ-Weight: 1
  QP 3
    Qtype: SP5,
    WRP: 1, Name: wrp-1
    CIR (%): 0, PIR (%): 100,
    WFQ-Mode: WERR, WFQ-Weight: 1
  QP 4
    Qtype: SP4,
    WRP: 1, Name: wrp-1
    CIR (%): 0, PIR (%): 100,
    WFQ-Mode: WERR, WFQ-Weight: 1
  QP 5
    Qtype: SP3,
    WRP: 1, Name: wrp-1
    CIR (%): 0, PIR (%): 100,
    WFQ-Mode: WERR, WFQ-Weight: 1
  QP 6

* QSP2 has all WRR schedulers.

<table>
<thead>
<tr>
<th>OmniSwitch</th>
<th>QSP1 (All-SP)</th>
<th>QSP2</th>
<th>QSP3</th>
<th>QSP4</th>
<th>QSP5 (All-WRR)</th>
<th>Custom QSP</th>
<th>Base QSP for Custom QSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS6360</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>QSP1, QSP2</td>
</tr>
<tr>
<td>OS6465</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>QSP1, QSP5</td>
</tr>
<tr>
<td>OS6560</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>QSP1, QSP5</td>
</tr>
<tr>
<td>OS6570M</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>OS6860/6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>QSP1, QSP5</td>
</tr>
<tr>
<td>OS6860N*</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>QSP1, QSP2</td>
</tr>
<tr>
<td>OS6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>QSP1, QSP2</td>
</tr>
<tr>
<td>OS6900-X72</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>QSP1, QSP 5</td>
</tr>
<tr>
<td>OS6900-V72/C32*</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>QSP1, QSP2</td>
</tr>
<tr>
<td>OS6900-X48C6/T48C6/X48C4E/V48C8*</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>QSP1, QSP2</td>
</tr>
<tr>
<td>OS9900</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>QSP1, QSP5</td>
</tr>
</tbody>
</table>
QoS Commands

show qos qsp

Qtype: SP2,
WRP: 1, Name: wrp-1
CIR (%): 0, PIR (%): 100,
WFQ-Mode: WERR, WFQ-Weight: 1
QP 7
Qtype: SP1,
WRP: 1, Name: wrp-1
CIR (%): 0, PIR (%): 100,
WFQ-Mode: WERR, WFQ-Weight: 1
QP 8
Qtype: SP0,
WRP: 1, Name: wrp-1
CIR (%): 0, PIR (%): 100,
WFQ-Mode: WERR, WFQ-Weight: 1

output definitions

QSP The QSet profile (QSP) ID number and name.
#Ports The number of ports to which this profile is attached.
#Queues The number of queues associated with this QSet. Currently there are eight queues for each QSet.
BW% The bandwidth percentage for the QSet. The bandwidth is shared between all the queues.
WRP Not supported in this release.
Name Not supported in this release.
Scheduler The type of scheduler, such as queue specific priority (Qspec) or strict priority.
Type Whether the QSP is static (predefined) or dynamic (user-configured). Refer to the table in the “Usage Guidelines” section for a list of the predefined QSPs and to determine whether user-configured QSPs are supported.
QP 1...8 The queue profile configuration for each QSet queue. The configuration for each of the individual queue profiles is defined by the QSP in use. For example, QSP 1 applies a different queue configuration than QSP 2, 3, or 4.

-> show qos qsp brief
<table>
<thead>
<tr>
<th>Profile</th>
<th>Name</th>
<th>#Ports</th>
<th>#Queues</th>
<th>BW(%)</th>
<th>Type</th>
<th>Base Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>qsp-1</td>
<td>58</td>
<td>8</td>
<td>100</td>
<td>Static</td>
<td>qsp-1</td>
</tr>
<tr>
<td>5</td>
<td>qsp-5</td>
<td>0</td>
<td>8</td>
<td>100</td>
<td>Static</td>
<td>qsp-5</td>
</tr>
<tr>
<td>6</td>
<td>qsp-6</td>
<td>0</td>
<td>8</td>
<td>100</td>
<td>Dynamic</td>
<td>qsp-5</td>
</tr>
</tbody>
</table>

output definitions

Profile The QSet profile (QSP) ID number.
Name The QSP name.
#Ports The number of ports to which this profile is attached.
#Queues The number of queues associated with this QSet. Currently there are eight queues for each QSet.
**output definitions (continued)**

**BW%**
The bandwidth percentage for the QSet. The bandwidth is shared between all the queues.

**Type**
Whether the QSP is static (predefined) or dynamic (user-configured). Refer to the table in the “Usage Guidelines” section for a list of the predefined QSPs and to determine whether user-configured QSPs are supported.

**Base Profile**
The profile on which the QSP is based. The profile number will differ for user-configured profiles.

```
-> show qos qsp detail

Legends: T (Type): S = Static, D = Dynamic

<table>
<thead>
<tr>
<th>QSAP Port</th>
<th>QSAP Type dQSI</th>
<th>ID Name</th>
<th>Parent</th>
<th>BW (%)</th>
<th>BW (%)</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Phy Port 1/1/1</td>
<td>qsp-1</td>
<td>Port 1/1/1</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Phy Port 1/1/2</td>
<td>qsp-1</td>
<td>Port 1/1/2</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Phy Port 1/1/3</td>
<td>qsp-1</td>
<td>Port 1/1/3</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/4</td>
<td>Phy Port 1/1/4</td>
<td>qsp-1</td>
<td>Port 1/1/4</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Phy Port 1/1/5</td>
<td>qsp-1</td>
<td>Port 1/1/5</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/6</td>
<td>Phy Port 1/1/6</td>
<td>qsp-1</td>
<td>Port 1/1/6</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/7</td>
<td>Phy Port 1/1/7</td>
<td>qsp-1</td>
<td>Port 1/1/7</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/8</td>
<td>Phy Port 1/1/8</td>
<td>qsp-1</td>
<td>Port 1/1/8</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/9</td>
<td>Phy Port 1/1/9</td>
<td>qsp-1</td>
<td>Port 1/1/9</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/10</td>
<td>Phy Port 1/1/10</td>
<td>qsp-1</td>
<td>VFL 1/0</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/11</td>
<td>Phy Port 1/1/11</td>
<td>qsp-1</td>
<td>Port 1/1/11</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>1/1/12</td>
<td>Phy Port 1/1/12</td>
<td>qsp-1</td>
<td>Port 1/1/12</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/1/27</td>
<td>Phy Port 2/1/27</td>
<td>qsp-1</td>
<td>Port 2/1/27</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>2/1/28</td>
<td>Phy Port 2/1/28</td>
<td>qsp-1</td>
<td>Port 2/1/28</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>2/1/29</td>
<td>Phy Port 2/1/29</td>
<td>qsp-2</td>
<td>VFL 2/0</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>2/1/30</td>
<td>Phy Port 2/1/30</td>
<td>qsp-1</td>
<td>Port 2/1/30</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>10</td>
<td>Log Linkagg 10</td>
<td>qsp-1</td>
<td>Linkagg 10</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>vf1-1/0</td>
<td>Log VFL 1/0</td>
<td>qsp-2</td>
<td>VFL 1/0</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>vf1-2/0</td>
<td>Log VFL 2/0</td>
<td>qsp-2</td>
<td>VFL 2/0</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
</tbody>
</table>
```

-> show qos qsp detail port 1/1/12

Legends: T (Type): S = Static, D = Dynamic

```
<table>
<thead>
<tr>
<th>QSAP Port</th>
<th>QSAP Type dQSI</th>
<th>ID Name</th>
<th>Parent</th>
<th>BW (%)</th>
<th>BW (%)</th>
<th>T</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/1/27</td>
<td>Phy Port 2/1/27</td>
<td>qsp-1</td>
<td>Port 2/1/27</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>2/1/28</td>
<td>Phy Port 2/1/28</td>
<td>qsp-1</td>
<td>Port 2/1/28</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>2/1/29</td>
<td>Phy Port 2/1/29</td>
<td>qsp-2</td>
<td>VFL 2/0</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>2/1/30</td>
<td>Phy Port 2/1/30</td>
<td>qsp-1</td>
<td>Port 2/1/30</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>10</td>
<td>Log Linkagg 10</td>
<td>qsp-1</td>
<td>Linkagg 10</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>vf1-1/0</td>
<td>Log VFL 1/0</td>
<td>qsp-2</td>
<td>VFL 1/0</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
<tr>
<td>vf1-2/0</td>
<td>Log VFL 2/0</td>
<td>qsp-2</td>
<td>VFL 2/0</td>
<td>100</td>
<td>100</td>
<td>S</td>
</tr>
</tbody>
</table>
```

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 36-88
QoS Commands

show qos qsp

| 1/1/12 | Phy | Port 1/1/12 | 1 | qsp-1 | Port 1/1/12 | 100 | 100 | S |

output definitions

- **QSAP Port**: The port number, link aggregate ID, or virtual fabric link (VFL) ID for the QSet attachment point (QSAP). A QSAP is a logical entity generated internally by the switch to identify the association between a QSet instance and a port, link aggregate, and VFL. The QSAP is not configurable at this time.

- **QSAP Type**: The type of QSAP port; Phy = physical (slot/port), Log = logical (linkagg ID or VFL ID).

- **dQSI**: The default QSet instance (dQSI) ID number. This number is generated internally by the switch to identify the QSI that is automatically assigned to each port, link aggregate, and VFL.

- **ID**: The QSet profile (QSP) ID number.

- **Name**: The QSP name.

- **QSAP Parent**: The QSAP parent ID number. If the parent ID is different than the QSAP ID, then the port is a member of a link aggregate or a VFL.

- **BW (%) Admin**: The administrative bandwidth percentage for the QSet. The administrative percentage is not configurable at this time.

- **BW (%) Oper**: The operational percentage of bandwidth as determined by the port speed. For a link aggregate, this value is the sum of the operational bandwidth percentages for the member ports.

- **T**: Whether the QSP type is static (S) or dynamic (D). Refer to the table in the “Usage Guidelines” section for a list of the static (predefined) QSPs and to determine whether dynamic (user-configured) QSPs are supported.

Release History

Release 7.2.1; command was introduced.

Related Commands

- **qos qsi qsp**: Changes the QSet profile association for a QSet instance.
- **show qos qsi**: Displays the QSet instance configuration.

MIB Objects

- `alcatelIND1VfcMIB`
- `alaVfcQsetProfileTable`
  - `alaVfcQSPId`
  - `alaVfcQSPName`
  - `alaVfcQSPBandwidthLimitValue`
  - `alaVfcQSPQueueCount`
  - `alaVfcQSPSchedulingMethod`
  - `alaVfcQSPStatsAdmin`
  - `alaVfcQSPAttachmentCount`
show qos wrp

Displays the Weighted Random Early Detection (WRED) profile (WRP) configuration for the switch.

```
show qos wrp [wrp_id | wrp_name] [detail [port chassis/slot/port[-port2]]] | slot slot | linkagg agg_id[-agg_id2]]
```

### Syntax Definitions

- **wrp_id**
  - A WRED profile (WRP) ID number. The valid range is 1.

- **wrp_name**
  - A WRED profile name.

- **detail**
  - Displays WRED profile configuration details for a port, slot, or link aggregate.

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number of a non-DCB (Data Center Bridging) port. Use a hyphen to specify a range of ports (1/5-10).

- **slot**
  - A slot number. Displays information for all non-DCB ports on the slot.

- **agg_id[-agg_id2]**
  - The link aggregate ID for a non-DCB aggregate. Use a hyphen to specify a range of IDs (10-15).

### Defaults

N/A

### Platforms Supported

Not supported in this release.

### Usage Guidelines

- This command is not supported on OmniSwitch 6900 DCB ports.
- Use the `wrp_id` or the `wrp_name` parameter to display information for a specific profile.
- Use the `detail` parameter to display additional profile information, such as the profile configuration associated with queues and ports.
- Use the `port slot/port, slot slot, and linkagg agg_id` parameters to display profile information associated with specific ports or link aggregates. These parameters are used in combination with the `detail` parameter.

### Examples

```
-> show qos wrp
WRP  1 (wrp-1)
  #Ports:  480, MTU:  1540
  Red
    Min-Th:  10, Max-Th:  50, Max-Pb:  36, Gain:  9
  Yellow
    Min-Th:  50, Max-Th:  90, Max-Pb:  30, Gain:  9
  Green
    Min-Th:  90, Max-Th: 100, Max-Pb:  24, Gain:  9
```
### QoS Commands

#### show qos wrp

```
-> show qos wrp 1 detail port 2/4
Port 2/4
  QSAP: Port 2/4, Parent: Port 2/4,
  WRP: 1, Name: wrp-1, Admin: Dis
  QSI Port 2/4
  QSP: 1, Name: qsp-1, Admin: Ena
  QI 1
    WRP: 1, Name: wrp-1, Admin: Dis
  QI 2
    WRP: 1, Name: wrp-1, Admin: Dis
  QI 3
    WRP: 1, Name: wrp-1, Admin: Dis
  QI 4
    WRP: 1, Name: wrp-1, Admin: Dis
  QI 5
    WRP: 1, Name: wrp-1, Admin: Dis
  QI 6
    WRP: 1, Name: wrp-1, Admin: Dis
  QI 7
    WRP: 1, Name: wrp-1, Admin: Dis
  QI 8
    WRP: 1, Name: wrp-1, Admin: Dis
```

### output definitions

<table>
<thead>
<tr>
<th>WRP</th>
<th>The WRED profile (WRP) ID number and name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>#Ports</td>
<td>The number of ports to which this profile is attached.</td>
</tr>
<tr>
<td>MTU</td>
<td>The MTU size.</td>
</tr>
<tr>
<td>Min-Th</td>
<td>The minimum queue threshold percentage for red, green, and yellow packets.</td>
</tr>
<tr>
<td>Max-Th</td>
<td>The maximum queue threshold percentage for red, green, and yellow packets.</td>
</tr>
<tr>
<td>Max-Pb</td>
<td>The maximum drop probability percentage for red, green, and yellow packets.</td>
</tr>
<tr>
<td>Gain</td>
<td>The gain value to smooth out the queue (1–15).</td>
</tr>
</tbody>
</table>

### Port

The physical slot and port number (or link aggregate ID for a logical port).

### QSAP

The QSet attachment point (QSAP). This is a logical entity used internally by the switch to identify the association between a QSet instance and a port or link aggregate. The QSAP is not configurable at this time.

### Parent

The QSAP ID for the parent QSAP, if any.

### WRP Name Admin

The WRED profile (WRP) ID number, name, and administrative status.

### QSI

The switch port associated with the QSet instance (QSI).

### QSP Name Admin

The QSet profile (QSP) ID number, name, and administrative status.

### QI 1...8

The WRP information for each of the QSet queues.
Release History

Release 7.2.1; command was introduced.

Related Commands

qos qsi qsp
Changes the QSet profile association for a QSet instance.
show qos qsi
Displays the QSet instance configuration.

MIB Objects

alcatelIND1VfcMIB
alaVfcWREDProfileTable
alaVfcWRPID
alaVfcWRPAdminState
alaVfcWRPName
alaVfcWRPGreenMinThreshold
alaVfcWRPGreenMaxThreshold
alaVfcWRPGreenMaxDropProbability
alaVfcWRPGreenGain
alaVfcWRPYellowMinThreshold
alaVfcWRPYellowMaxThreshold
alaVfcWRPYellowMaxDropProbability
alaVfcWRPYellowGain
alaVfcWRPRedMinThreshold
alaVfcWRPRedMaxThreshold
alaVfcWRPRedMaxDropProbability
alaVfcWRPRedGain
alaVfcWRPMTU
alaVfcWRPAttachmentCount
alaVfcWRPLastChange
alaVfcWRPRowStatus
**show qos qsi**

Displays the QSet instance (QSI) configuration for the switch. A QSI is a logical set of eight egress queues associated with each port, link aggregate (LAG) ID, and virtual fabric link (VFL).

**show qos qsi [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2] | vf-link vfl_id] [detail | summary]**

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port[-port2]</td>
<td>The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).</td>
</tr>
<tr>
<td>agg_id[-agg_id2]</td>
<td>The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).</td>
</tr>
<tr>
<td>vfl_id</td>
<td>The VFL ID (1/0). <em>This parameter option is supported only on the OmniSwitch 6860 and OmniSwitch 6865.</em></td>
</tr>
<tr>
<td>detail</td>
<td>Displays additional queue information for the instance.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays summary information for the instance.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, displays the entire QSI configuration for the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `port slot/port, slot slot, linkagg agg_id, and vf-link vfl_id` parameters to display the QSI information associated with specific ports, link aggregates, or VFLs. These parameters can also be combined with the `detail` or `summary` parameters.

**Examples**

```
-> show qos qsi port 1/1/1
Port 1/1/1
  QSAF: Port 1/1/1, Parent: Port 1/1/1
  QSI  Port 1/1/1
    QSP: 1, Name: qsp-1,
    WRP: 1, Name: wrp-1, Admin: Dis, Oper: Dis
    Stats
      Admin: Dis, Oper: Dis, Interval: 60
    BW
```
Admin (%): 100, Oper (%): 100

-> show qos qsi port 1/1/54
Port 1/1/54
    QSAP: Port 1/1/54, Parent:     VFL 1/0
    QSI   Port 1/1/54
    QSP:  2, Name:        qsp-2,
    WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
    Stats
         Admin: Dis, Oper: Dis, Interval:    60
    BW
        Admin (%): 100, Oper (%): 100

-> show qos qsi vf-link 1/0
VFL 1/0
    QSAP:     VFL 1/0, Parent:     VFL 1/0
    QSI      VFL 1/0
    QSP:  1, Name:        qsp-1,
    WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
    Stats
         Admin: Dis, Oper: Dis, Interval:    60
    BW
        Admin (%): 100, Oper (%): 100

-> show qos qsi port 1/1/1 detail
Port 1/1/1
    QSAP:    Port 1/1/1, Parent:    Port 1/1/1
    QSI      Port 1/1/1
    QSP:  1, Name:        qsp-1,
    WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
    Stats
         Admin: Dis, Oper: Dis, Interval:    60
    BW
        Admin (%): 100, Oper (%): 100
    QI  1
    Qtype: SP7,
    WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
         CIR
             Admin (%):   0, Oper (%):   0
         PIR
             Admin (%): 100, Oper (%): 100
    QI  2
    Qtype: SP6,
    WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
         CIR
             Admin (%):   0, Oper (%):   0
         PIR
             Admin (%): 100, Oper (%): 100
    QI  3
    Qtype: SP5,
    WRP:  1, Name:        wrp-1, Admin: Dis, Oper: Dis
         CIR
             Admin (%):   0, Oper (%):   0
         PIR
             Admin (%): 100, Oper (%): 100
    QI  4
    Qtype: SP4,
Admin (%): 0, Oper (%): 0
PIR
Admin (%): 100, Oper (%): 100

QI 5
Qtype: SP3,
WRP: l, Name: wrp-1, Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (%): 0
PIR
Admin (%): 100, Oper (%): 100

QI 6
Qtype: SP2,
WRP: l, Name: wrp-1, Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (%): 0
PIR
Admin (%): 100, Oper (%): 100

QI 7
Qtype: SP1,
WRP: l, Name: wrp-1, Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (%): 0
PIR
Admin (%): 100, Oper (%): 100

QI 8
Qtype: SP0,
WRP: l, Name: wrp-1, Admin: Dis, Oper: Dis
CIR
Admin (%): 0, Oper (%): 0
PIR
Admin (%): 100, Oper (%): 100

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QSAP</td>
<td>The port number, link aggregate ID, or virtual fabric link (VFL) ID for the QSet attachment point (QSAP). A QSAP is a logical entity generated internally by the switch to identify the association between a QSet instance and a port, link aggregate, and VFL. The QSAP is not configurable at this time.</td>
</tr>
<tr>
<td>Parent</td>
<td>The parent QSAP ID. If the parent ID is different than the QSAP ID, then the port is a member of a link aggregate or VFL.</td>
</tr>
<tr>
<td>QSI</td>
<td>The QSet instance (QSI) ID number, internally generated by the switch.</td>
</tr>
<tr>
<td>QSP, Name</td>
<td>The QSet profile (QSP) ID number and name associated with the QSI.</td>
</tr>
<tr>
<td>WRP, Name, Admin, Oper</td>
<td>Not supported in this release.</td>
</tr>
<tr>
<td>Stats, Admin, Oper, Interval</td>
<td>The QSI administrative status, operational status, and time interval for statistics collection.</td>
</tr>
<tr>
<td>BW Admin (%)</td>
<td>The administrative percentage of bandwidth (currently not user-configurable).</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

**BW Oper (%)**
The operational percentage of bandwidth as determined by the port speed. For a link aggregate, this value is the sum of the operational bandwidth percentages for the member ports.

**QI 1–8**
The queue scheduling and bandwidth configuration for each QSI queue. These values are determined by which one of the QSet profiles (QSP 1–4) is associated with the QSI.

```
-> show qos qsi port 1/1/20 summary
Legends: * indicates port is misconfigured.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Port</th>
<th>Name</th>
<th>Mode</th>
<th>Parent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1/1/20</td>
<td>qsp-1</td>
<td>NDCB</td>
<td>1/1/20</td>
</tr>
</tbody>
</table>

-> show qos qsi vf-link 1/0 summary
Legends: * indicates port is misconfigured.

<table>
<thead>
<tr>
<th>Profile</th>
<th>Port</th>
<th>Name</th>
<th>Mode</th>
<th>Parent</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>vfl-1/0</td>
<td>qsp-2</td>
<td>NDCB</td>
<td>vfl-1/0</td>
</tr>
</tbody>
</table>
```

**output definitions**

**Port**
The physical slot and port number (or link aggregate ID or VFL ID for a logical port).

**Profile #, Name**
The QSet profile (QSP) ID number and name associated with the QSI.

**Mode**
The QSI operating mode (**NDCB** or **DCB**). This mode determines whether Data Center Bridging (DCB) profiles or QSet profiles (non-DCB) are applied to the QSI instance. DCB and QSet profiles are mutually exclusive in that if the OmniSwitch Data Center software license is installed, only DCB profiles are applied.

**Parent**
The parent QSAP ID. If the parent ID is different than the QSAP ID, then the port is a member of a link aggregate or VFL.

**Release History**

Release 7.1.1; command was introduced.
Release 7.2.1; output display modified for the OmniSwitch 6900.
Release 7.2.1.R02; output display modified for the OmniSwitch 6900.
Release 8.3.1; **vf-link** and **summary** parameters added.

**Related Commands**

- **qos qos qsp**
  Changes the QSet profile association for a QSet instance.

- **show qos qsi stats**
  Displays packet count statistics collected for a specific QSet instance.
**MIB Objects**

alcatelIND1VfcMIB
alaVfcQsetInstanceTable
  alaVfcQsetId
  alaVfcQsetQsapId
  alaVfcQsetAdminState
  alaVfcQsetQSPId
  alaVfcQsetQSPName
  alaVfcQsetSchedulingMethod
  alaVfcQsetStatsAdmin
  alaVfcQsetStatsOper
alaVfcQInstanceTable
  alaVfcQInstanceQId
  alaVfcQInstanceCIRBandwidthLimitValue
  alaVfcQInstancePIRBandwidthLimitValue
  alaVfcQInstanceCIROperationalBandwidthLimitValue
  alaVfcQInstancePIROperationalBandwidthLimitValue
  alaVfcQInstanceStatsAdmin
  alaVfcQInstanceStatsOper
show qos qsi stats

Displays statistics for the QSet instance (QSI) queues that are associated with non-DCB (NDCB) ports.

```bash
show qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} stats [bytes | rate [bytes]]
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).

- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-15).

- **bytes**
  - Displays the total number of bytes (instead of packets) that flow through the QSI queues.

- **rate**
  - Displays the number of packets-per-second that flow through the QSI queues.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>bytes</td>
</tr>
<tr>
<td>rate</td>
<td>bytes</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The specified port or link aggregate must have statistics collection enabled.
- Use the `port slot/port` or `linkagg agg_id` parameters to display QSI statistics associated with specific ports or link aggregates.
- It is possible to combine the `bytes` parameter with the `rate` parameter to display the number of bytes-per-second that flow through the QSI queues. For example, `show qos qsi port 1/20 stats rate bytes`.
- Statistics are displayed on a per-queue basis for each port. There are eight queues associated with a single QSet instance. Each queue is identified with a queue ID (1–8). Each port and link aggregate is associated with one QSet instance.
### Examples

```plaintext
-> show qos qsi port 1/20 stats

<table>
<thead>
<tr>
<th>Port</th>
<th>Q</th>
<th>Tx</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/20</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>8</td>
<td>9984</td>
<td>0</td>
</tr>
</tbody>
</table>

-> show qos qsi port 1/20 stats bytes

<table>
<thead>
<tr>
<th>Port</th>
<th>Q</th>
<th>Tx</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/20</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>8</td>
<td>987424</td>
<td>0</td>
</tr>
</tbody>
</table>

-> show qos qsi port 1/20 stats rate

<table>
<thead>
<tr>
<th>Port</th>
<th>Q</th>
<th>Tx/s</th>
<th>Drop/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/20</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>8</td>
<td>7</td>
<td>0</td>
</tr>
</tbody>
</table>

-> show qos qsi port 1/20 stats rate bytes

<table>
<thead>
<tr>
<th>Port</th>
<th>Q</th>
<th>Tx/s</th>
<th>Drop/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/20</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/20</td>
<td>8</td>
<td>694</td>
<td>0</td>
</tr>
</tbody>
</table>
```
output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The slot and port number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q</td>
<td>The QSet queue ID number (1–8) associated with the QoS (non-DCB) port.</td>
</tr>
<tr>
<td>Total Tx</td>
<td>Total packets or bytes transmitted.</td>
</tr>
<tr>
<td>Total Drop</td>
<td>Total packets or bytes dropped.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

- **qos qsi stats**: Enables or disables statistics collection for a DCB or non-DCB port.
- **clear qos qsi stats**: Clears statistics collected for one or more QSet instances.

MIB Objects

- **alaVfcQInstanceTable**
  - **alaVfcQInstancePacketsEnqueued**
  - **alaVfcQInstanceBytesEnqueued**
  - **alaVfcQInstancePacketsDropped**
  - **alaVfcQInstanceBytesDropped**
**show qos qsi ecn-stats**

Displays the Enhanced Congestion Notification (ECN) statistics of a port or linkagg.

```
show qos qsi [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2] ecn-stats [bytes | rate [bytes]]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-15).
- `bytes` Displays the total number of bytes (instead of packets) that flow through the QSI queues.
- `rate` Displays the number of packets-per-second that flow through the QSI queues.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The specified port or link aggregate must have statistics collection enabled.
- Use the `port slot/port` or `linkagg agg_id` parameters to display QSI statistics associated with specific ports or link aggregates.
- It is possible to combine the `bytes` parameter with the `rate` parameter to display the number of bytes-per-second that flow through the QSI queues. For example, `show qos qsi port 1/20 ecn-stats rate bytes`.
- Statistics are displayed on a per-queue basis for each port. There are eight queues associated with a single QSet instance. Each queue is identified with a queue ID (1–8). Each port and link aggregate is associated with one QSet instance.
- ECN Marked, Q-Full Drop packet statistics are not available.
- ECN Marked, WRED Drop, Q-Full Drop bytes statistics are not available.
Examples

-> show qos qsi linkagg 100 ecn-stats rate
Legends: ECN Marked, Q-Full Drop stats are not available

<table>
<thead>
<tr>
<th>Linkagg</th>
<th>Q</th>
<th>Tx</th>
<th>ECN Marked Tx</th>
<th>WRED Drop</th>
<th>Q-Full Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/100</td>
<td>1</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/100</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/100</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/100</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/100</td>
<td>5</td>
<td>3</td>
<td></td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>

-> show qos qsi port 1/1/2A ecn-stats bytes
Legends: ECN Marked, WRED Drop, Q-Full Drop bytes stats are not available

<table>
<thead>
<tr>
<th>Port</th>
<th>Q</th>
<th>Tx</th>
<th>ECN Marked Tx</th>
<th>WRED Drop</th>
<th>Q-Full Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2A</td>
<td>1</td>
<td>1708940</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/2A</td>
<td>2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/2A</td>
<td>3</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/2A</td>
<td>4</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

output definitions

- **Linkagg**: The link aggregate ID.
- **Port**: The port number.
- **Q**: The egress queue ID (1-8) associated with the port.
- **Tx**: The total packets or bytes transmitted.
- **ECN Marked Tx**: The number of ECN marked packets or bytes transmitted. ECN Marked Tx packets and bytes statistics are not available.
- **WRED Drop**: The number of WRED (Non ECT) packets/bytes dropped. WRED drop bytes statistics are not available.
- **Q-Full Drop**: (Total packets/bytes dropped) - (WRED packets/bytes dropped). Q-Full drop packets and bytes statistics are not available.

Release History

Release 8.7R2; command introduced.

Related Commands

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos ecnp import ecnp</td>
<td>Creates a custom Enhanced Congestion Notification (ECN) profile in a non-Data Center Bridging (NDCB) mode.</td>
</tr>
</tbody>
</table>

MIB Objects

<table>
<thead>
<tr>
<th>object</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
show qos qsi wred-stats

Displays the Weighted Random Early Detection (WRED) statistics for the QSet instance.

show qos qsi {port chassis/slot/port[-port2] | slot slot | linkagg agg_id[-agg_id2]} wred-stats [rate | bytes]

Syntax Definitions

chassis
The chassis identifier.

slot/port[-port2] The slot and port number of a non-DCB (Data Center Bridging) port. Use a hyphen to specify a range of ports (1/5-10).

agg_id[-agg_id2] The link aggregate ID number of a non-DCB aggregate. Use a hyphen to specify a range of IDs (10-15).

rate Displays the number of packets per second.

bytes Displays the total number of bytes.

Defaults

By default, displays the total number of packets for all the QSI queues.

Platforms Supported

Not supported in this release.

Usage Guidelines

- This command is not supported on OmniSwitch 6900 DCB ports.
- Use the port slot/port, slot slot, and linkagg agg_id parameters to display QSI statistics associated with specific ports or link aggregates.
- This command displays the total number of packets or bytes.

Examples

-> show qos qsi port 1/2 wred-stats
* OS6900 WRED Per Q stats not supported, Tx stats not supported

<table>
<thead>
<tr>
<th>Port</th>
<th>Q Drop</th>
<th>Yellow</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

-> show qos qsi port 1/1 wred-stats rate
* OS6900 WRED Per Q stats not supported, Tx stats not supported

<table>
<thead>
<tr>
<th>Port</th>
<th>Q Drop/s</th>
<th>Drop/s</th>
<th>Drop/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
-> show qos qsi port 1/1 wred-stats bytes
* OS6900  WRED Per Q stats not supported, Tx stats not supported

<table>
<thead>
<tr>
<th>Port</th>
<th>Q</th>
<th>Drop</th>
<th>Drop</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**output definitions**

- **Port**: The switch port.
- **Q**: The egress queue ID (1–8) associated with the port.
- **Green TX, Green Drop**: The number of green packets or bytes transmitted and dropped.
- **Yellow TX, Yellow Drop**: The number of yellow packets or bytes transmitted and dropped.
- **Red TX, Red Drop**: The number of red packets or bytes transmitted and dropped.

**Release History**

Release 7.2.1.R01; WRED per Q stats not supported; Tx stats not supported.

**Related Commands**

- **show qos qsi**: Displays the QSet instance configuration.
- **clear qos qsi stats**: Clears statistics collected for one or more QSet instances.

**MIB Objects**

- `alcatelIND1VfcMIB`
- `alaVfcQInstanceTable`
- `alaVfcQInstanceQId`
- `alaVfcQInstanceGreenPacketsAccepted`
- `alaVfcQInstanceGreenBytesAccepte`
- `alaVfcQInstanceGreenPacketsDropped`
- `alaVfcQInstanceGreenBytesDropped`
- `alaVfcQInstanceYellowPacketsAccepted`
- `alaVfcQInstanceYellowBytesAccepted`
- `alaVfcQInstanceYellowPacketsDropped`
- `alaVfcQInstanceYellowBytesDropped`
- `alaVfcQInstanceRedPacketsAccepted`
- `alaVfcQInstanceRedBytesAccepted`
- `alaVfcQInstanceRedPacketsDropped`
- `alaVfcQInstanceRedBytesDropped`
**show qos qsp system-default**

Displays the name and ID of the QSet profile (QSP) that serves as the default system QSP when the switch is running in the non-DCB (NDCB) mode.

```
show qos qsp system-default
```

**Syntax Definitions**

N/A

**Defaults**

By default, QSP 1 is assigned to each QSet instance.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
+-------+-------+-------+-------+-------+-------+-------+-------+
| 6360  | 6465  | 6560  | 6570M | 6860  | 6860N | 6865  | 6900  |
+-------+-------+-------+-------+-------+-------+-------+-------+
|    No |    No |    No |    No | Yes   | Yes   | Yes   | No    |
|-------+-------+-------+-------+-------+-------+-------+-------+
|     6900 V72/C32 |     6900 X48C6/T48C6 |     6900 X48C4E/V48C8/C32E/T24C2 |     9900 |
+-------+-------+-------+-------+-------+-------+-------+-------+
|     No |     No |     No |     No |     No |     No |     No |     No |
+-------+-------+-------+-------+-------+-------+-------+-------+
```

**Usage Guidelines**

- The switch is operating in the NDCB mode when the OmniSwitch Data Center software license is *not* installed on the switch.
- The switch is operating in the Data Center Bridging (DCB) mode when the OmniSwitch Data Center software license is installed on the switch. Configuring the system default profile is not supported in the DCB mode.

**Examples**

```
-> show qos qsp system-default
NDCB Default QSP profile : 1 (qsp-1)
```

**Release History**

Release 8.3.1; command introduced.
QoS Commands

show qos qsp system-default

Related Commands

cos qsp system-default

Configures the default QSet profile for the switch.

MIB Objects

alcatelIND1VfcMIB

alaVfcSystemDefaultQsetQSPName

alaVfcSystemDefaultQsetQSPId
clear qos qsi stats

Clears QSet instance (QSI) statistics.

clear qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} stats

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (1\5). Use a hyphen to specify a range of ports (1/5-10).
- **agg_id[-agg_id2]**: The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900 X48C4E/N48C8/</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **port slot/port** and **linkagg agg_id** parameters to clear QSI statistics associated with specific ports or link aggregates.
- QSI statistics can only be cleared on ports or link aggregates that have statistics collection enabled.

Examples

-> clear qos qsi port 1/1/2 stats
-> clear qos qsi port 1/1/10-15 stats
-> clear qos qsi linkagg 5 stats
-> clear qos qsi linkagg 10-15 stats

Release History

Release 7.1.1; command was introduced.
QoS Commands

Related Commands

`show qos qsi stats`  Displays QSet instance statistics.

MIB Objects

alcatelIND1VfcMIB
alaVfcQsapTable
  alaVfcQsapClearStats
  alaVfcQsapQpId
**qos qsp dcb import**

Imports a Data Center Bridging profile (DCP) to a new or previous custom profile.

```
qos qsp dcb {dcp_id | dcp_name} import qsp dcb {import_dcp_id | import_dcp_name} [802.3x-pause]
```

```
no qos qsp dcb {dcp_id | dcp_name}
```

### Syntax Definitions

- **dcp_id**: A DCB custom profile ID. The valid custom profile ID range is 12 through 128.
- **dcp_name**: The DCB profile name.
- **import_dcp_id**: The ID of the DCB profile to import. The valid profile ID range is 1–11 to specify a predefined profile and 12–128 to specify a custom profile.
- **import_dcp_name**: The name of the DCB profile to import.
- **802.3x-pause**: Makes the profile pause-ready. When enabled, the Priority based Flow Control (PFC) is lossy for all traffic classes in the profile and they cannot be changed to lossless.

### Defaults

By default the **802.3x-pause** flag is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The new DCB profile must be unique and not contain the same name and ID of an existing DCB profile.
- On an OmniSwitch 6900-Q32, only import DCB profile 8 to create a custom profile. Do not use any of the other pre-defined profiles to create a custom profile.
- Use the **no** form of the command to remove an existing custom DCB profile from the switch configuration.
- The pre-defined DCB profiles from 1 to 11 cannot be removed from the switch configuration.
- A custom profile attached to a port cannot be removed from the switch configuration. In this case, the profile must be disassociated from the port before being removed.
Use the **802.3x-pause** tag to enable pause-ready on the profile. When enabled, the PFC is lossy for all traffic classes in the profile and they cannot be changed to lossless. This type of custom profile is created to support legacy PAUSE frames on ports to which the profile is applied. However, before applying the custom profile to a port, disable PFC TLV and PFC willing on the port.

**Examples**

```
-> qos qsp dcb 33 import qsp dcb 8
-> qos qsp dcb lossyETS import qsp 10
-> qos qsp dcb 34 import qsp dcb 7 802.3x-pause
-> no qsp dcb 33
```

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show qos qsp dcb` Displays the configured DCB profile and the traffic classes associated to the DCB profile.
- `show qos qsi stats` Displays the queue statistics for DCB and Non-DCB (NDCB) ports.
- `clear qos qsi dcb pfc stats` Clears the port statistics.

**MIB Objects**

- `alaDcbxDCProfileTable`
- `alaDcbxDCPId`
- `alaDcbxDCPName`
- `alaDcbxDCPTemplateDCPId`
- `alaDcbxDCPTemplateDCPName`
- `alaDcbxDCP8023xPauseReady`
- `alaDcbxDCPRowStatus`
**qos qsp dc**

Modifies the Data Center Bridging (DCB) traffic class attributes of a DCB profile.

```bash
qos qsp dc {dcp_id | dcp_name} tc tc_num {pfc flow-type { ll | nll} | pfc link-delay allowance | min-bw % | max-bw % | recommended bw %}
```

### Syntax Definitions

**dcp_id**
A DCB custom profile ID. The valid custom profile ID range is 12 through 128.

**dcp_name**
The DCB custom profile name.

**tc_num**
The traffic class number in the DCB profile.

**ll**
Designates traffic class as lossless.

**nll**
Designates traffic class as non-lossless (lossy).

**allowance**
Link delay allowance value for PFC.

**min-bw %**
Sets the minimum bandwidth guaranteed for the Enhanced Transmission Selection (ETS) traffic class.

**max-bw %**
Sets the maximum bandwidth guaranteed for the Strict Priority (SP) traffic class.

**recommended bw %**
Sets the recommended minimum bandwidth for the traffic class.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The **pfc flow-type** option is used to change a traffic class from lossless (ll) to lossy (nll) or from lossy (nll) to lossless (ll).
- The **pfc link-delay** option sets the actual headroom for the traffic class. An incorrect setting can result in traffic loss.
- The **min-bw** option sets the minimum bandwidth guaranteed for the ETS traffic class.
- The **max-bw** option sets the maximum bandwidth guaranteed for the SP traffic class.
- The **recommended bw** option sets the recommended minimum bandwidth for the traffic class.
**Examples**

```
-> qos qsp dcbb 11 tc 0 min-bw 3
-> qos qsp dcbb lossyETS tc 1 min-bw 12
-> qos qsp dcbb lossyETS tc 2 pfc flow-type ll
-> qos qsp dcbb 11 tc 0 recommended bw 3
```

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

```
show qos qsp dcbb
```

Displays the configured DCB profiles and the traffic classes associated to the DCB profile.

**MIB Objects**

```
alaDcbxDCPTTrafficClassTable
  alaDcbxDCPTCDCPId
  alaDcbxDCPTCTrafficClass
  alaDcbxDCPTCDCPName
  alaDcbxDCPTCPFCTrafficFlow
  alaDcbxDCPTCPFCLinkDelay
  alaDcbxDCPTCMinimumBandwidth
  alaDcbxDCPTCMaximumBandwidth
  alaDcbxDCPTCRecommendedBandwidth
```
**qos qsp dcb tc-numbering**

Modifies the traffic class (TC) numbering for custom profiles.

```
qos qsp dcb {dcp_id | dcp_name} tc-numbering tc_num
```

**Syntax Definitions**

- `dcp_id`: A DCB custom profile ID. The valid custom profile ID range is 12 through 128.
- `dcp_name`: The DCB custom profile name.
- `tc_num`: Enter the traffic class numbering sequence for the DCB profile.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The command can be used to modify the traffic class numbering for the custom profiles.
- The numbering must be assigned in ascending order. For example, a profile with TCs numbered 0, 1, 2, can be changed to 1, 5, 7.
- The number of TCs specified must match the number of TCs in the profile.

**Examples**

```
-> qos qsp dcb 11 tc-numbering 1 5 7 9
```

**Release History**

Release 7.3.1; command was introduced.
Related Commands

show qos qsp dcb

Displays the configured DCB profiles and the traffic classes associated to the DCB profile.

MIB Objects

alaDcbxDProfileTable
  alaDcbxDCTCDCPName
  alaDcbxDCTCSPresent
**qos qsi qsp dcb**

Assigns a DCB profile to a port or link aggregate.

```
qos qsi {port chassis[slot/port[-port2]} | linkagg agg_id[-agg_id2]} qsp dcb {dcp_id | dcb_name}
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- **agg_id[-agg_id2]**: The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
- **dcp_id**: DCB profile ID. DCB profile ID 11 through 128 refers to the custom profiles. DCB profile ID 1 through 10 refers to the predefined profiles.
- **dcp_name**: DCB profile name.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When a DCB profile is assigned to a link aggregate, the profile is applied to all the ports associated with the linkagg.
- Avoid configuring different profiles for each port of the link aggregate.
- The command will not work if the link aggregate is associated with 1Gig port. Different combination of ports (10G and 40G) are allowed in a link aggregate.

**Examples**

- `-> qos qsi port 1/11 qsp dcb lossyETS`
- `-> qos qsi port 1/11 qsp dcb 7`

**Release History**

Release 7.3.1; command was introduced.
Related Commands

*show qos qsp dcb* Displays the configured DCB profiles and the traffic classes associated with the DCB profile.

MIB Objects

*alaDcbxPortInstanceEntry*
- *alaDcbxPIAdminDCPId*
- *alaDcbxPIAdminDCPName*
**qos qsi dcb dcbx version**

Selects the version of the DCB Exchange protocol (DCBX) to apply to the specified DCB port.

```
qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb dcbx version {ieee | cee | auto}
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- `agg_id[-agg_id2]` The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
- `ieee` Selects IEEE 802.1Qaz DCBX.
- `cee` Selects Converged Enhanced Ethernet DCBX 1.01.
- `auto` Automatically detects the DCBX version used by the peer switch.

**Defaults**

By default, the DCB port is configured to automatically use the DCBX version detected from the peer.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Initially, the IEEE version of DCBX is run on the port until the switch detects the peer is running the CEE version. At that point, the switch will stop IEEE DCBX and start to run the CEE version.

**Examples**

- `-> qos qsi port 1/10 dcb dcbx version ieee`
- `-> qos qsi port 1/10 dcb dcbx version cee`
- `-> qos qsi port 1/11 dcb dcbx version auto`

**Release History**

Release 7.3.3; command was introduced.
**Related Commands**

- `qos qsi dcb dcbx admin-state` enables or disables DCBX functionality on the port.
- `qos qsi dcb dcbx ets` enables or disables application Type, Length, Value (TLV) transmission on a per-port basis.
- `qos qsi dcb dcbx pfc` enables or disables config-TLV, defense mode, and willing bit for PFC on a per-port basis.
- `show qos qsi dcb dcbx` displays the DCBX configuration and status for the specified port.

**MIB Objects**

- `alaDcbxPortInstanceEntry`
- `alaDcbxPIDCBXVersion`
**qos qsi dcb dcbx admin-state**

Enables or disables DCB exchange protocol (DCBX) functionality on a per port basis.

```
qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb dcbx admin-state {enable | disable}
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- **agg_id[-agg_id2]**: The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
- **enable**: Enables the DCBX functionality on the port.
- **disable**: Disables the DCBX functionality on the port.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>dcbx admin-state</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The DCBX admin-state, enables or disables DBCX TLVs and negotiation on a port.

**Examples**

- `-> qos qsi port 1/10 dcb dcbx admin-state enable`
- `-> qos qsi port 1/10 dcb dcbx admin-state disable`

**Release History**

Release 7.3.1; command was introduced.
Related Commands

- `qos qsi dcbl dcbx version`: Selects the version of DCBX to apply to the specified DCB port.
- `qos qsi dcbl dcbx ets`: Enables or disables application Type, Length, Value (TLV) transmission on a per port basis.
- `qos qsi dcbl dcbx pfc`: Enables or disables config-TLV, defense mode, and willing bit for PFC on a per port basis.
- `show qos qsi dcbl dcbx`: Displays the configured ports in the system and the related DCBX information.

MIB Objects

- `alaDcbxPortInstanceEntry`
  - `alaDcbxPIIIfIndex`
  - `alaDcbxPIDCBXAdmin`
**qos qsi dcb dcbx ets**

Enables or disables config-TLV, recommended-TLV, and the willing bit for ETS on a per-port basis.

```
qos qsi {port chassis/slot/port[1-port2] | linkagg agg_id[1-agg_id2]} dcb dcbx ets [config-tlv {enable | disable} | recommend-tlv {enable | disable} | willing {yes | no}]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[1-port2]` The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- `agg_id[1-agg_id2]` The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
- `config-tlv enable` Enables the transmission of ETS configuration TLVs.
- `config-tlv disable` Disables the transmission of ETS configuration TLVs.
- `recommend-tlv enable` Enables the transmission of ETS recommended TLVs.
- `recommend-tlv disable` Disables the transmission of ETS recommended TLVs.
- `yes` Sets the willing bit to on in the TLVs.
- `no` Sets the willing bit to off in the TLVs.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>config-tlv {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>ets recommend-tlv {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>willing {yes</td>
<td>no}</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the option `ets config-tlv` to enable or disable the transmission of ETS configuration TLVs. To use this option, DCBX must be enabled on the port.

- Use the option `ets recommended-tlv` to enable or disable the transmission of ETS recommended TLVs. To use this option, DCBX must be enabled on the port.
Use the option **ets willing** to set the willing bit on the TLVs. This option is used when the DCBX is enabled on the port and the ETS configuration TLV is sent on the port.

**Examples**

- `-> qos qsi port 1/1-10 dcb dcbx ets config-tlv disable`
- `-> qos qsi port 1/11 dcb dcbx ets recommended-tlv disable`
- `-> qos qsi linkagg 5 dcb dcbx ets willing no`

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **qos qsi dcb dcbx version**  Selects the version of DCBX to apply to the specified DCB port.
- **qos qsi dcb dcbx admin-state**  Enables or disables DCBX functionality for the port.
- **qos qsi dcb dcbx pfc**  Enables or disables config-TLV, defense mode, and willing bit for PFC on a per port basis.
- **show qos qsi dcb dcbx**  Displays the configured ports in the system and the related DCBX information.
- **show qos qsi dcb ets**  Displays the configured ports in the system and the related DCBX ETS and ETS traffic class information.

**MIB Objects**

- `lldpXdot1dcbxConfigETSConfigurationTable`
- `lldpXdot1dcbxConfigETSRecommendationTable`
- `lldpXdot1dcbxLocETSBasicConfigurationTable`
  - `lldpXdot1dcbxConfigETSConfigurationTxEnable`
  - `lldpXdot1dcbxConfigETSRecommendationTxEnable`
  - `lldpXdot1dcbxLocETSSCOnWilling`
**qos qos dcb dcbx pfc**

Enables or disables config-TLV, defense mode, and willing for PFC on a per port basis.

```
qos qos {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb dcbx pfc [config-tlv {enable | disable} | defense {enable | disable} | willing {yes | no}]
```

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- `agg_id[-agg_id2]` The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
- `config-tlv enable` Enables the transmission of PFC configuration TLVs.
- `config-tlv disable` Disables the transmission of PFC configuration TLVs.
- `defense enable` Enables the defense mode for the PFC.
- `defense disable` Disables the defense mode for the PFC.
- `willing yes` Allows the PFC to negotiate with the network.
- `willing no` Stops the PFC from negotiating with the network.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>pfc config-tlv</td>
<td>enable</td>
</tr>
<tr>
<td>pfc defense</td>
<td>enable</td>
</tr>
<tr>
<td>pfc willing</td>
<td>yes</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the option `pfc config-tlv` to enable or disable the transmission of PFC configuration TLVs. To use this option, DCBX must be enabled on the port.
- Use the option `ets willing` to allow the PFC to negotiate with the network.
QoS Commands

Examples

-> qos qsi port 1/1-10 dcb dcbx pfc config-tlv disable
-> qos qsi port 1/11 dcb dcbx pfc defense disable
-> qos qsi linkagg 5 dcb dcbx pfc willing no

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi dcbx pfc Displays the configured ports in the system and the related DCBX PFC information.
show qos pfc-lossless-usage Displays the usage of the PFC lossless traffic class on the switch.
show qos qsi dcb pfc stats Displays the traffic statistics per port and per traffic class.

MIB Objects

lldpXdot1dcbxConfigPFCTable
  lldpXdot1dcbxConfigPFCTxEnable
  alaDcbxPIPFCDefense
  lldpXdot1dcbxLocPFCWilling
**show qos qsp dcb**

Displays the configured DCB profiles and the traffic classes associated with the DCB profile.

**show qos qsp dcb [dcp_id | dcp_name] [tc tc_num]**

---

### Syntax Definitions

- **dcp_id**: DCB profile ID. DCB profile ID 11–128 refers to the custom profiles. DCB profile ID 1–0 refers to the predefined profiles.
- **dcp_name**: DCB profile name.
- **tc_num**: The traffic class associated to the DCB profile. The valid range is 0–7.

---

### Defaults

N/A

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- This command displays the details of the configured DCB profile.
- Use the **tc** option to display the traffic classes associated to the DCB profile.

---

### Examples

```
-> show qos qsp dcb
```

**Legends: Prio TC Map:**

Represents the priority to traffic class mapping; begins with priority 0 on the left and displays the traffic class it belongs to.

<table>
<thead>
<tr>
<th>ETS</th>
<th>Priority</th>
<th>PFC</th>
<th>Max Template-DCP</th>
<th>802.3x</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>TC Map</td>
<td>Cap TC</td>
<td>Name</td>
<td>Pause-Ready</td>
</tr>
<tr>
<td>#</td>
<td></td>
<td></td>
<td>#</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>dcp-1</td>
<td>00001122 8 8 1 dcp-1</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>dcp-2</td>
<td>00112338 8 8 2 dcp-2</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>dcp-3</td>
<td>00112348 8 8 3 dcp-3</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>dcp-4</td>
<td>10234568 8 8 4 dcp-4</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>dcp-5</td>
<td>10234568 8 8 5 dcp-5</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>dcp-6</td>
<td>10234568 8 8 6 dcp-6</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
### Output Definitions

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>TC Priorities</th>
<th>BW</th>
<th>BW</th>
<th>Sched BW</th>
<th>Sched Mode</th>
<th>LinkDelay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dft_1</td>
<td>0 4567</td>
<td>0</td>
<td>100</td>
<td>SP</td>
<td>nLL</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Dft_1</td>
<td>1 23</td>
<td>50</td>
<td>100</td>
<td>ETS</td>
<td>LL</td>
<td>80*</td>
</tr>
<tr>
<td>1</td>
<td>Dft_1</td>
<td>2 01</td>
<td>50</td>
<td>100</td>
<td>ETS</td>
<td>LL</td>
<td>60</td>
</tr>
</tbody>
</table>

### Legends: Linkdelay shown in KB.

- * denotes user modified value

### Output Definitions

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>TC Priorities</th>
<th>BW</th>
<th>BW</th>
<th>Sched BW</th>
<th>Sched Mode</th>
<th>LinkDelay</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Dft_1</td>
<td>0 4567</td>
<td>0</td>
<td>100</td>
<td>SP</td>
<td>nLL</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>Dft_1</td>
<td>1 23</td>
<td>50</td>
<td>100</td>
<td>ETS</td>
<td>LL</td>
<td>80*</td>
</tr>
<tr>
<td>1</td>
<td>Dft_1</td>
<td>2 01</td>
<td>50</td>
<td>100</td>
<td>ETS</td>
<td>LL</td>
<td>60</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `qos qsp dcb import` Imports a data center profile to a new or old custom DCB profile.
- `clear qos qsi stats` Modifies the Data Center Bridging Capabilities Exchange Protocols (DCBX) control portion of a DCB profile.
- `qos qsp dcb tc` Modifies the Data Center Bridging (DCB) attributes of a DCB profile.
- `qos qsp dcb tc-numbering` Modifies the priority of traffic class mapping the custom profiles.
- `clear qos qsi dcb pfc stats` Clears the port statistics.

**MIB Objects**

- `alaDcbxDCProfileTable`
  - `alaDcbxDCPId`
  - `alaDcbxDCPName`
  - `alaDcbxDCPPriorityTCMap`
  - `alaDcbxDCPPFCCap`
  - `alaDcbxDCPETSTrafficClassesSupported`
  - `alaDcbxDCPTemplateDCPId`
  - `alaDcbxDCPTemplateDCPName`
  - `alaDcbxDCP8023xPauseReady`
- `alaDcbxDCPTrafficClassTable`
  - `alaDcbxDCPTCDCPId`
  - `alaDcbxDCPTCDCPName`
  - `alaDcbxDCPTCTrafficClass`
  - `alaDcbxDCPTCPriorityMap`
  - `alaDcbxDCPTCMinimumBandwidth`
  - `alaDcbxDCPTCMaximumBandwidth`
  - `alaDcbxDCPTCTrafficScheduler`
  - `alaDcbxDCPTCRecommendedBandwidth`
  - `alaDcbxDCPTCRecommendedTrafficScheduler`
  - `alaDcbxDCPTCPFCTrafficFlow`
  - `alaDcbxDCPTCPFCLinkDelay`
**show qos qsi dcb dcbx**

Displays the DCBX port configuration and status.

```
show qos qsi [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] dcb dcbx [status]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- `agg_id[-agg_id2]` A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
- `status` Displays the DCBX operational status for the port.

**Defaults**

By default, the DCBX configuration is displayed for all ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `port slot/port` or `linkagg agg_id`, parameters to display information for a specific port or link aggregate.
- Use the `status` option to display the status information of the DCBX related to the port.

**Examples**

```
-> show qos qsi port 1/1-5 dcb dcbx
```

<table>
<thead>
<tr>
<th>Port</th>
<th>DCP Name</th>
<th>DCBX Ver</th>
<th>DCBX Admin</th>
<th>Stats Ver</th>
<th>Stats Admin</th>
<th>PFC Ver</th>
<th>PFC Admin</th>
<th>PFC Cfg</th>
<th>PFC Reco</th>
<th>ETS TLV</th>
<th>ETS Will</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>8</td>
<td>AUTO</td>
<td>Ena</td>
<td>Dis</td>
<td>Ena</td>
<td>Yes</td>
<td>Ena</td>
<td>Ena</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1/2</td>
<td>8</td>
<td>AUTO</td>
<td>Ena</td>
<td>Dis</td>
<td>Ena</td>
<td>Yes</td>
<td>Ena</td>
<td>Ena</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1/3</td>
<td>8</td>
<td>AUTO</td>
<td>Ena</td>
<td>Dis</td>
<td>Ena</td>
<td>Yes</td>
<td>Ena</td>
<td>Ena</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>1/4</td>
<td>8</td>
<td>AUTO</td>
<td>Ena</td>
<td>Dis</td>
<td>Ena</td>
<td>Yes</td>
<td>Ena</td>
<td>Ena</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The DCB slot and port number or link aggregate ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCP</td>
<td>The DCB profile ID assigned to the port.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the DCB profile assigned to the port.</td>
</tr>
<tr>
<td>DCBX Ver</td>
<td>The version of DCBX running on the port (CEE, IEEE, or AUTO).</td>
</tr>
<tr>
<td>DCBX Admin</td>
<td>Indicates the administrative status of DCBX on the port.</td>
</tr>
<tr>
<td>Stats Admin</td>
<td>Indicates if statistics collection is enabled or disabled on the port.</td>
</tr>
<tr>
<td>PFC Defense</td>
<td>Indicates the status of PFC defense (Ena or Dis). Applies when PFC negotiation fails. If enabled then PFC becomes disabled but traffic still flows. If disabled then the PFC local configuration remains on the port.</td>
</tr>
<tr>
<td>PFC TLV</td>
<td>Indicates whether the IEEE 802.1 organizationally defined PFC TLV transmission is allowed on a given LLDP transmission capable port.</td>
</tr>
<tr>
<td>PFC Will</td>
<td>Indicates whether or not the port is willing to accept the PFC configuration from a remote peer.</td>
</tr>
<tr>
<td>Cfg TLV</td>
<td>Indicates whether or not ETS configuration TLV transmission is allowed on a port.</td>
</tr>
<tr>
<td>Reco TLV</td>
<td>Indicates whether or not ETS configuration TLV transmission is allowed on a port.</td>
</tr>
<tr>
<td>ETS Will</td>
<td>Indicates whether or not the port is willing to accept the recommended ETS configuration from a remote peer.</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The DCB slot and port number or link aggregate ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCBX Oper</td>
<td>Indicates the operational status of DCBX on the port.</td>
</tr>
<tr>
<td>Local Oper Changed</td>
<td>Identifies if the local configuration is different from the configuration imported from the DCB profile applied to the port.</td>
</tr>
<tr>
<td>Error</td>
<td>Indicates if there is an error condition.</td>
</tr>
<tr>
<td>Local Oper Ver</td>
<td>The version of DCBX running on the local port (CEE, IEEE, or AUTO).</td>
</tr>
<tr>
<td>Remote Oper Ver</td>
<td>The version of DCBX running on the remote port (CEE, IEEE, or AUTO).</td>
</tr>
<tr>
<td>Action</td>
<td>Indicates the action taken as a result of the status.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.3.1; command was introduced.
Release 7.3.3; fields added to display the version of DCBX (IEEE or CEE).

**Related Commands**

- `qos qsi qsp dcb`: Assigns a DCB profile to a port or link aggregate.
- `qos qsi dcb dcbx version`: Configures the version of DCBX to run on the port (IEEE or CEE).
- `qos qsi dcb dcbx admin-state`: Enables or disables DCBX functionality on a port basis.
- `qos qsi stats`: Enables or disables statistics collection.

**MIB Objects**

- `alaDcbxPortInstanceEntry
  laaDcbxPIIfIndex
  laaDcbxP IDCBXAdmin
  laaDcbxP IDCBXOper
  laaDcbxPIAdminDCPID
  laaDcbxPIAdminDCPName
  laaDcbxPILocalModified
  laaDcbxPIPPCDefense
  laaDcbxPIPFSClear
  laaDcbxPIStatus
  laaDcbxPIActionTaken
  laaDcbxPIRowStatus
  laaDcbxPIDCBXVersion
  laaDcbxPIDCBXVersionOper`

- `alaDcbxPortInstanceGroup
  laaDcbxPIDCBXAdmin
  laaDcbxPIDCBXOper
  laaDcbxPIAdminDCPID
  laaDcbxPIAdminDCPName
  laaDcbxPILocalModified
  laaDcbxPIPPCDefense
  laaDcbxPIPFSClear
  laaDcbxPIStatus
  laaDcbxPIActionTaken
  laaDcbxPIRowStatus
  laaDcbxPIDCBXVersion
  laaDcbxPIDCBXVersionOper`
show qos qsi dcb ets

Displays the configured ports in the system and the related DCBX ETS and ETS traffic class information.

`show qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb ets [tc [tc_num]]`

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port[-port2]`: The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).
- `agg_id[-agg_id2]`: A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).
- `tc_num`: Enter the traffic class for which the information needs to be displayed. The valid range is 0–7.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

Use the `tc_num` option to display the DCBX ETS information for a specific traffic class.

**Examples**

```
-> show qos qsi port 1/1 dcb ets
Legends: Prio TC Map:
        Represents the priority to traffic class mapping;
        begins with priority 0 on the left and displays the traffic class it belongs to.
        * indicates port oper status is different than the configured status

<table>
<thead>
<tr>
<th>Loc-Adm</th>
<th>Loc-Adm</th>
<th>Loc-Oper</th>
<th>Loc-Oper</th>
<th>Rem-Oper</th>
<th>Rem-Oper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prio</td>
<td>Max</td>
<td>Prio</td>
<td>Max</td>
<td>Prio</td>
<td>Max</td>
</tr>
<tr>
<td>Port</td>
<td>TC Map</td>
<td>TC CBS</td>
<td>Will TC Map</td>
<td>TC CBS</td>
<td>Will TC Map</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
<td>----------</td>
<td>-----------</td>
<td>---------</td>
<td>----------</td>
</tr>
<tr>
<td>1/1</td>
<td>00111222 3</td>
<td>Dis</td>
<td>Yes</td>
<td>00111222 3</td>
<td>Dis</td>
</tr>
</tbody>
</table>
```
### output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>Configured DCB ports.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Loc-Adm Prio TC Map</th>
<th>Indicates the traffic class to which the priority is to be assigned.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loc-Adm Max TC</td>
<td>Indicates the number of traffic classes supported.</td>
</tr>
<tr>
<td>Loc-Adm CBS</td>
<td>Indicates the status of the credit-based shaper traffic support.</td>
</tr>
<tr>
<td>Loc-Adm Will</td>
<td>Indicates if the local system is willing to accept the ETS configuration recommended by the remote system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Loc-Oper Prio TC Map</th>
<th>Indicates the traffic class to which the priority belongs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loc-Oper Max TC</td>
<td>Indicates the number of traffic classes supported in the local system.</td>
</tr>
<tr>
<td>Loc-Oper CBS</td>
<td>Indicates if the credit-based shaper traffic is supported on the local system.</td>
</tr>
<tr>
<td>Loc-Oper Will</td>
<td>Indicates if the credit-based shaper traffic selection is supported on the local system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rem-Oper Prio TC Map</th>
<th>Indicates the priority that is assigned to a traffic class.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rem-Oper Max TC</td>
<td>Indicates the number of traffic classes supported in the remote system.</td>
</tr>
<tr>
<td>Rem-Oper CBS</td>
<td>Indicates if the credit-based shaper traffic selection is supported on the remote system.</td>
</tr>
<tr>
<td>Rem-Oper Will</td>
<td>Indicates if the remote system is willing to accept the ETS configuration recommended by the remote system.</td>
</tr>
</tbody>
</table>

**Legends:** * indicates port oper status is different than the configured status

```
-> show qos qsi port 1/1 dcb ets tc
```

### output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>Configured DCB ports.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>TC</th>
<th>Indicates the traffic class to which the priority belongs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loc-Adm Priorities</td>
<td>Indicates the priority assigned to the traffic class in the local system.</td>
</tr>
<tr>
<td>Loc-Adm BW</td>
<td>Indicates the bandwidth assignment to the traffic class in the local system.</td>
</tr>
<tr>
<td>Loc-Adm Sched</td>
<td>Indicates the traffic selection assignment to the traffic class in the local system.</td>
</tr>
<tr>
<td>Loc-Adm Reco BW</td>
<td>Indicates the traffic class to bandwidth assignment in the local system.</td>
</tr>
<tr>
<td>Loc-Adm Reco Sched</td>
<td>Indicates the traffic class to traffic selection assignment in the local system.</td>
</tr>
<tr>
<td>Loc-Oper Priorities</td>
<td>Indicates the priority assigned to the traffic class in the local system.</td>
</tr>
<tr>
<td>Loc-Oper BW</td>
<td>Indicates the bandwidth assigned to the traffic class in the local system.</td>
</tr>
</tbody>
</table>
**QoS Commands**  
show qos qos dcb ets

---

**output definitions (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loc-Oper Sched</td>
<td>Indicates the traffic class to traffic selection assignment in the local system.</td>
</tr>
<tr>
<td>Loc-Oper Reco BW</td>
<td>Indicates the traffic class to bandwidth assignment in the local system.</td>
</tr>
<tr>
<td>Loc-Oper Reco Sched</td>
<td>Indicates the priority to traffic selection assignment in the local system.</td>
</tr>
<tr>
<td>Rem-Oper Priorities</td>
<td>Indicates the priority assigned to the traffic class in the remote system.</td>
</tr>
<tr>
<td>Rem-Oper BW</td>
<td>Indicates the traffic class to bandwidth assignment in the remote system.</td>
</tr>
<tr>
<td>Rem-Oper Sched</td>
<td>Indicates the traffic class to traffic selection assignment in the remote system.</td>
</tr>
<tr>
<td>Rem-Oper Reco BW</td>
<td>Indicates the traffic class to bandwidth assignment in the remote system.</td>
</tr>
<tr>
<td>Rem-Oper Reco Sched</td>
<td>Indicates the priority to traffic selection assignment in the remote system.</td>
</tr>
</tbody>
</table>

---

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

qos qos dcb dcbx ets  
Enables or disables config-tlv, recommended-tlv, and willing for ETS on a per port basis.
MIB Objects

lldpXdot1dcbxAdminETSConPriorityAssignmentTable
lldpXdot1dcbxAdminETSBasicConfigurationTable
lldpXdot1dcbxLocETSConPriorityAssignmentTable
lldpXdot1dcbxLocETSBasicConfigurationTable
lldpXdot1dcbxRemETSConPriorityAssignmentTable
lldpXdot1dcbxRemETSBasicConfigurationTable
  lldpV2LocPortIfIndex
  lldpXdot1dcbxAdminETSConPriTrafficClass
  lldpXdot1dcbxAdminETSConTrafficClassesSupported
  lldpXdot1dcbxAdminETSConCreditBasedShaperSupport
  lldpXdot1dcbxAdminETSConWilling
  lldpXdot1dcbxLocETSConPriTrafficClass
  lldpXdot1dcbxLocETSConTrafficClassesSupported
  lldpXdot1dcbxLocETSConCreditBasedShaperSupport
  lldpXdot1dcbxLocETSConWilling
  lldpXdot1dcbxRemETSConPriTrafficClass
  lldpXdot1dcbxRemETSConTrafficClassesSupported
  lldpXdot1dcbxRemETSConCreditBasedShaperSupport
  lldpXdot1dcbxRemETSConWilling
  lldpXdot1dcbxAdminETSConTrafficClassBandwidthTable
  lldpXdot1dcbxAdminETSConTrafficSelectionAlgorithmTable
  lldpXdot1dcbxAdminETSRecoTrafficClassBandwidthTable
  lldpXdot1dcbxAdminETSRecoTrafficSelectionAlgorithmTable
  lldpXdot1dcbxLocETSConTrafficClassBandwidthTable
  lldpXdot1dcbxLocETSConTrafficSelectionAlgorithmTable
  lldpXdot1dcbxLocETSRecoTrafficClassBandwidthTable
  lldpXdot1dcbxLocETSRecoTrafficSelectionAlgorithmTable
  lldpXdot1dcbxRemETSConTrafficClassBandwidthTable
  lldpXdot1dcbxRemETSConTrafficSelectionAlgorithmTable
  lldpXdot1dcbxRemETSRecoTrafficClassBandwidthTable
  lldpXdot1dcbxRemETSRecoTrafficSelectionAlgorithmTable
   lldpV2LocPortIfIndex
   lldpXdot1dcbxAdminETSConTrafficClass
   lldpXdot1dcbxAdminETSConTrafficClassBandwidth
   lldpXdot1dcbxAdminETSConTrafficSelectionAlgorithm
   lldpXdot1dcbxAdminETSRecoTrafficClassBandwidth
   lldpXdot1dcbxAdminETSRecoTrafficSelectionAlgorithm
   lldpXdot1dcbxLocETSConTrafficClassBandwidth
   lldpXdot1dcbxLocETSConTrafficSelectionAlgorithm
   lldpXdot1dcbxLocETSRecoTrafficClassBandwidth
   lldpXdot1dcbxLocETSRecoTrafficSelectionAlgorithm
   lldpXdot1dcbxRemETSConTrafficClassBandwidth
   lldpXdot1dcbxRemETSConTrafficSelectionAlgorithm
   lldpXdot1dcbxRemETSRecoTrafficClassBandwidth
   lldpXdot1dcbxRemETSRecoTrafficSelectionAlgorithm
   lldpXdot1dcbxRemETSRecoTrafficSelectionAlgorithm
**show qos qsi dcbx pfc**

Displays the configured ports in the system and the related DCBX PFC information.

**show qos qsi {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} dcb pfc**

---

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).

- **agg_id[-agg_id2]**
  - A link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

If there is no PFC TLV received from the remote end, then the remote information will be blank.

---

**Examples**

-> show qos qsi port 4/1-2 dcb pfc

Legends: * indicates port oper status is different than the configured status

<table>
<thead>
<tr>
<th>Port</th>
<th>Loc-Adm Priorities</th>
<th>Loc-Adm MBC</th>
<th>Loc-Oper Priorities</th>
<th>Loc-Oper MBC</th>
<th>Rem-Oper Priorities</th>
<th>Rem-Oper MBC</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/1*</td>
<td>0467</td>
<td>No</td>
<td>Yes</td>
<td>3</td>
<td>01</td>
<td>No</td>
</tr>
<tr>
<td>4/2*</td>
<td>23</td>
<td>No</td>
<td>No</td>
<td>3</td>
<td>-</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**output definitions**

- **Port**
  - Configured DCB ports.

- **Loc-Adm Priorities**
  - Indicates the priority for which PFC is enabled or disabled.

- **Loc-Adm MBC**
  - Indicates if the local system is capable of bypassing MACsec processing when MACsec is disabled.
Release History

Release 7.3.1; command was introduced.

Related Commands

```
qos qsi dcb dcbx pfc
```

Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.

MIB Objects

```
lldpXdot1dcbxAdminPFCEnableTable
lldpXdot1dcbxAdminPFCBasicTable
lldpXdot1dcbxLocPFCEnableTable
lldpXdot1dcbxLocPFCBasicTable
lldpXdot1dcbxRemPFCEnableTable
lldpXdot1dcbxRemPFCBasicTable
   ldpV2LocPortIfIndex
   ldpXdot1dcbxAdminPFCEnableEnabled
   ldpXdot1dcbxAdminPFCWilling
   ldpXdot1dcbxAdminPFCCap
   ldpXdot1dcbxLocPFCEnableEnabled
   ldpXdot1dcbxLocPFCMBC
   ldpXdot1dcbxLocPFCWilling
   ldpXdot1dcbxLocPFCCap
   ldpXdot1dcbxRemPFCEnableEnabled
   ldpXdot1dcbxRemPFCMBC
   ldpXdot1dcbxRemPFCWilling
```
<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldpXdotlmdcbxRemPFCCap</td>
</tr>
</tbody>
</table>
**show qos pfc-lossless-usage**

Displays the usage of the PFC lossless traffic class on the switch.

```bash
-> show qos pfc-lossless-usage
Lossless Priorities in use : 55,
Lossless Priorities reserved : 60,
Lossless Priorities available : 73
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the PFC lossless traffic class usage on the switch.

**Examples**

```bash
-> show qos pfc-lossless-usage
Lossless Priorities in use : 55,
Lossless Priorities reserved : 60,
Lossless Priorities available : 73
```

**output definitions**

- **Lossless Priorities in use**: Indicates the number of PFC lossless priorities in use in the system.
- **Lossless Priorities reserved**: Indicates the number of PFC lossless priorities in reserve in the system.
- **Lossless Priorities available**: Indicates the number of priorities available to be configured as PFC lossless.

**Release History**

Release 7.3.1; command was introduced.
**Related Commands**

`qos qsi decb debx pfc`  
Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.

**MIB Objects**

- `alaDcbxConfig`
  - `alaDcbxPfcLLPrioritiesUsed`
  - `alaDcbxPfcLLPrioritiesReserved`
  - `alaDcbxPfcLLPrioritiesAvailable`
show qos qsi dcb pfc stats

Displays the Priority Flow Control (PFC) statistics for the specified DCB port.

show qos qsi [port chassis/slot/port[-port2]] dcb pfc stats

Syntax Definitions

chassis
The chassis identifier.

slot/port[-port2]
The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Statistics are displayed on a per-traffic class (TC) basis.

Examples

-> show qos qsi port 1/11 dcb pfc stats

Legends: displays packet count

<table>
<thead>
<tr>
<th>Port</th>
<th>Q</th>
<th>TC</th>
<th>TX (req)</th>
<th>RX (ind)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/11</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/11</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/11</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/11</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/11</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/11</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
QoS Commands

show qos qsi dcb pfc stats

1/11 7 2 0 0

output definitions

| Port | The DCB port number. |
| Q    | The 802.1p priority number (0–7). This number is mapped to a traffic class (TC) based on the DCB profile assigned to the port. |
| TC   | Indicates the traffic class to which the priority belongs. |
| Priority | Indicates the priority of the DCB port. |
| PFC TX (req) | Total count of PFC packets transmitted. |
| PFC RX (ind) | Total count of PFC packets received. |

Release History

Release 7.3.1; command was introduced.

Related Commands

- qos qsi dcb debx pfc Enables or disables config-tlv, defense mode, and willing for PFC on a per port basis.
- clear qos qsi dcb pfc stats Clears the port statistics.

MIB Objects

alaDcbxPIPPriorityTable
  alaDcbxPIPrioIfIndex
  alaDcbxPIPrioTC
  alaDcbxPIPrioPriority
  alaDcbxPIPrioPFCPacketsTransmitted
  alaDcbxPIPrioPFCPacketsReceived
clear qos qsi dcb pfc stats

Clears the DCB PFC queue statistics.

clear qos qsi {port chassis/slot/port[-port2]} dcb pfc stats

Syntax Definitions

chassis
The chassis identifier.

slot/port[-port2]
The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the slot/port parameter to clear queue statistics associated with specific ports.

Examples

-> clear qos qsi port 2/1 dcb pfc stats

Release History

Release 7.3.1; command was introduced.

Related Commands

show qos qsi stats Displays the queue statistics for DCB and NDCB ports.

MIB Objects

alaVfcQsetInstanceTable
alaVfcQsetStatsClear
**qos ecnp import ecnp**

Creates a custom Enhanced Congestion Notification (ECN) profile in a non-Data Center Bridging (NDCB) mode.

```
qos ecnp {cust_ecnp_id | cust_ecnp_name} import ecnp {ecnp_id | ecnp_name}
```

```
no qos ecnp {cust_ecnp_id | cust_ecnp_name}
```

---

**Syntax Definitions**

- **cust_ecnp_id**: ECN custom profile ID. The valid custom profile ID range is 2–16.
- **cust_ecnp_name**: The custom ECN profile name.
- **ecnp_id**: The ID of the ECN profile to import. Only ECN profile ID 1 can be used to create a custom profile.
- **ecnp_name**: The name of the ECN profile to import. Only ECNP profile name ecnp-1 can be used to create a custom profile.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Only ECNP profile ID: 1, name: ecnp-1 can be used to create a custom profile.
- Use the **no** form of the command to remove an existing custom ECN profile from the switch configuration.
- A custom ECN profile attached to a port cannot be removed from the switch configuration. In this case, the profile must be disassociated from the port before being removed.
- Ensure no ECN profile is being used by any QSI (Qset Instance) before deleting it. Detach the ECN profile from QSI before deleting it.
- ECN is supported only for IP unicast traffic flows.

---

**Examples**

```
-> qos ecnp 3 import ecnp 1
-> qos ecnp ecnptest import ecnp-1
-> no qos ecnp 3
```
**Release History**

Release 8.7R2; command introduced.

**Related Commands**

- `show qos ecnp` Displays the ECN configuration parameters for a port or a link aggregate.
- `show qos qsi ecn-stats` Displays the ECN statistics of a port or linkagg.

**MIB Objects**

alaVfcECNProfileTable
- alaVfcECNProfileName
- alaVfcECNProfileTemplateId
- alaVfcECNProfileTemplateName
- alaVfcECNProfileRowStatus
**qos ecnp value**

Configures the minimum and maximum queue threshold value of a custom Enhanced Congestion Notification Profile (ECNP).

```
qos ecnp {cust_ecnp_id | cust_ecnp_name} {min-threshold min_threshold_value | max-threshold max_threshold_value} value
```

### Syntax Definitions

- **cust_ecnp_id**: ECN custom profile ID.
- **cust_ecnp_name**: The custom ECN profile name.
- **min_threshold_value**: The minimum queue threshold value of a custom ECNP. The range is 0–100.
- **max_threshold_value**: The maximum queue threshold value of a custom ECNP. The range is 0–100.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>min_threshold_value</td>
<td>50</td>
</tr>
<tr>
<td>max_threshold_value</td>
<td>100</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Minimum threshold value cannot be greater the configured maximum threshold value.

### Examples

- `-> qos ecnp ecnptest min-threshold 10`
- `-> qos ecnp 3 max-threshold 90`
- `-> qos ecnp 3 min-threshold 20 max-threshold 75`

### Release History

Release 8.7R2; command introduced.
Related Commands

show qos ecnp  Displays the ECN configuration parameters for a port or a link aggregate.
show qos qsi ecn-stats  Displays the ECN statistics of a port or linkagg.

MIB Objects

alaVfcECNProfileTable
  alaVfcECNProfileName
  alaVfcECNProfileMinThreshold
  alaVfcECNProfileMaxThreshold
qos qsp ecn-profile

Assigns a custom ECNP to a custom QSet profile (QSP).

```
qos qsp {cust_qsp_id | cust_qsp_name} ecn-profile {cust_ecnp_id | cust_ecnp_name}
```

### Syntax Definitions

- **cust_qsp_id**: A QSet custom profile ID. The valid custom profile ID range is 3–8.
- **cust_qsp_name**: The custom QSet profile name.
- **cust_ecnp_id**: ECN custom profile ID.
- **cust_ecnp_name**: The custom ECN profile name.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

- `-> qos qsp qsptest ecn-profile encptest`
- `-> qos qsp 6 ecn-profile 3`

### Release History

Release 8.7R2; command introduced.
Related Commands

- `show qos ecnp` Displays the ECN configuration parameters for a port or a link aggregate.
- `show qos qsi ecn-stats` Displays the ECN statistics of a port or link aggregate.

MIB Objects

alaVfcECNProfileTable
  alaVfcECNProfileName
  alaVfcECNProfileTemplateId
  alaVfcECNProfileTemplateName
  alaVfcECNProfileRowStatus
**qos qsi qp ecn**

Enables or disables ECN functionality for the queue of a port or linkagg.

```
qos qsi {port chassis/slot/port[-port2] | slot slot | linkagg agg_id[-agg_id2]} qp q_num ecn admin-state {enable | disable}
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number to associate with the QSet. Use a hyphen to specify a range of ports (3/1-10).

- **slot**
  - The slot number.

- **agg_id[-agg_id2]**
  - The link aggregate ID to associate with the QSet. Use a hyphen to specify a range of IDs (10-20).

- **q_num**
  - The queue number. The range is 1–8.

- **enable**
  - Enables the ECNP for the queue.

- **disable**
  - Disables the ECNP for the queue.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-state</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When enabled, marking of ECT congested packets on the selected egress queue is enabled on the configured port only. ECN can only be activated for lower priority queues 5–8.

### Examples

- `-> qos qsi port 1/1/31 qp 5 ecn admin-state enable`
- `-> qos qsi port 1/1/31 qp 5 ecn admin-state disable`

### Release History

Release 8.7R2; command introduced.
Related Commands

- **show qos ecnp**
  Displays the ECN configuration parameters for a port or a link aggregate.

- **show qos qsi ecn-stats**
  Displays the ECN statistics of a port or link aggregate.

MIB Objects

- `alaVfcQInstanceTable`
- `alaVfcQInstanceECNAadminState`
show qos ecnp

Displays ECN configuration parameters for a port or a link aggregate.

show qos ecnp [ecnp_id | ecnp_name] [detail | port chassis/slot/port[-port2] | slot | linkagg agg_id[-agg_id2]]

**Syntax Definitions**

- **ecnp_id**
  - The ECN profile ID.

- **ecnp_name**
  - The ECN profile name.

- **detail**
  - Displays ECN configuration details for a specific port or a link aggregate.

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (1/5). Use a hyphen to specify a range of ports (1/5-10).

- **agg_id[-agg_id2]**
  - The link aggregate ID. Use a hyphen to specify a range of IDs (10-15).

**Defaults**

By default, displays the entire QSI configuration for the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **detail** parameter to display additional profile information for all ports and link aggregates.

**Examples**

```plaintext
-> show qos ecnp
ECNP 1 (ecnp-1)
#Ports: 135
  Green
    Min-Th: 50, Max-Th: 100, Max-Pb: 24, Gain: 9

-> show qos ecnp detail port 1/1/31A
Port 1/1/31A
  QSAP: Port 1/1/31A, Parent: Port 1/1/31A,
  ECNP: 1, Name: ecnp-1
  QSI Port 1/1/31A
    QSP: 1, Name: qsp-sp
```
QoS Commands

show qos ecnp

QI 1
  ECNP: 1, Name: ecnp-1, Admin: Dis
QI 2
  ECNP: 1, Name: ecnp-1, Admin: Dis
QI 3
  ECNP: 1, Name: ecnp-1, Admin: Dis
QI 4
  ECNP: 1, Name: ecnp-1, Admin: Dis
QI 5
  ECNP: 1, Name: ecnp-1, Admin: Dis
QI 6
  ECNP: 1, Name: ecnp-1, Admin: Dis
QI 7
  ECNP: 1, Name: ecnp-1, Admin: Ena
QI 8
  ECNP: 1, Name: ecnp-1, Admin: Dis

-> show qos ecnp detail linkagg 1

Linkagg 1
  QSAP: Linkagg 1, Parent: Linkagg 1,
  ECNP: 1, Name: ecnp-1
  QSI Linkagg 1
  QSP: 1, Name: qsp-sp
  QI 1
    ECNP: 1, Name: ecnp-1, Admin: Dis
  QI 2
    ECNP: 1, Name: ecnp-1, Admin: Dis
  QI 3
    ECNP: 1, Name: ecnp-1, Admin: Dis
  QI 4
    ECNP: 1, Name: ecnp-1, Admin: Dis
  QI 5
    ECNP: 1, Name: ecnp-1, Admin: Dis
  QI 6
    ECNP: 1, Name: ecnp-1, Admin: Dis
  QI 7
    ECNP: 1, Name: ecnp-1, Admin: Dis
  QI 8
    ECNP: 1, Name: ecnp-1, Admin: Ena

output definitions

ECNP
  The ECN profile (ECNP) ID and name.
#Ports
  The number of ports to which this profile is attached
Min-Th
  The minimum queue threshold for packets.
Max-Th
  The maximum queue threshold for packets.
Max-Pb
  The maximum drop probability percentage for packets.
Gain
  The queue gain (a numeric value used to determine the instantaneous average queue length)
Port/Linkagg
  The physical slot and port number (or link aggregate ID for a logical port)
QSAP
  The QSet Attachment Point (QSAP). This is a logical entity used internally by the switch to identify the association between a QSet instance and a port or link aggregate.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent</td>
<td>The QSAP ID for a parent QSAP, if any.</td>
</tr>
<tr>
<td>QSI</td>
<td>The switch port associated with the QSet Instance (QSI).</td>
</tr>
<tr>
<td>QSP Name</td>
<td>The QSet profile (QSP) ID number, name.</td>
</tr>
<tr>
<td>QI</td>
<td>The ECNP information for each of the QSet queues.</td>
</tr>
<tr>
<td>Admin</td>
<td>The ECN admin state for a QSet queue (Enable/Disable).</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.7R2; command introduced.

**Related Commands**

- `show qos ecnp` Displays the ECN configuration parameters for a port or a link aggregate.
- `show qos qsi ecn-stats` Displays the ECN statistics of a port or link aggregate.

**MIB Objects**

- `alaVfcECNProfileName`
- `alaVfcECNProfileTemplateName`
- `alaVfcECNProfileTemplateId`
- `alaVfcECNProfileMaxThreshold`
- `alaVfcECNProfileMinThreshold`
- `alaVfcECNProfileRowStatus`
This chapter describes the CLI commands used for policy management in the switch. The Quality of Service (QoS) software in the switch uses policy rules for classifying incoming flows and deciding how to treat outgoing flows. A policy rule is made up of a policy condition and a policy action. Policy rules may be created on the switch through CLI or SNMP commands, or they may be created through the PolicyView GUI application on an attached LDAP server.

Rules created through PolicyView cannot be modified through the CLI; however, you can create policies in the CLI that take precedence over policies created through PolicyView.

Refer to Chapter 36, “QoS Commands,” for information about commands used to configure QoS software.

MIB information for the QoS policy commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>ALCATEL-INDI-QOS-MIB.mib</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>alaQoSMIB</td>
</tr>
</tbody>
</table>

Some of the commands listed here are not currently supported on one or more platforms. See command descriptions in this chapter and check release notes for information about commands that are not supported.

The QoS Policy commands are listed here:

### Policy commands
- policy rule
-  ict message-type priority
- policy list
- policy list rules
- policy condition
- policy action
- show policy action
- show policy condition
- show active policy rule
- show policy rule
- show policy validity period
- show active policy list
- show policy list
- show policy ipv4-summary
- show policy ipv6-summary

### Group commands
- policy network group
- policy service
- policy service group
- policy mac group
- policy port group
- policy map group
- show policy network group
- show policy mac group
- show policy port group
- show policy map group
- show policy service
- show policy service group
<table>
<thead>
<tr>
<th>Condition commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy condition</td>
</tr>
<tr>
<td>policy condition source ip</td>
</tr>
<tr>
<td>policy condition source ipv6</td>
</tr>
<tr>
<td>policy condition destination ip</td>
</tr>
<tr>
<td>policy condition destination ipv6</td>
</tr>
<tr>
<td>policy condition multicast ip</td>
</tr>
<tr>
<td>policy condition source network group</td>
</tr>
<tr>
<td>policy condition destination network group</td>
</tr>
<tr>
<td>policy condition multicast network group</td>
</tr>
<tr>
<td>policy condition source ip-port</td>
</tr>
<tr>
<td>policy condition destination ip-port</td>
</tr>
<tr>
<td>policy condition source tcp-port</td>
</tr>
<tr>
<td>policy condition destination tcp-port</td>
</tr>
<tr>
<td>policy condition source udp-port</td>
</tr>
<tr>
<td>policy condition destination udp-port</td>
</tr>
<tr>
<td>policy condition ethertype</td>
</tr>
<tr>
<td>policy condition established</td>
</tr>
<tr>
<td>policy condition tcpflags</td>
</tr>
<tr>
<td>policy condition service</td>
</tr>
<tr>
<td>policy condition service group</td>
</tr>
<tr>
<td>policy condition icmptype</td>
</tr>
<tr>
<td>policy condition icmpcode</td>
</tr>
<tr>
<td>policy condition ip-protocol</td>
</tr>
<tr>
<td>policy condition ipv6</td>
</tr>
<tr>
<td>policy condition flow-label</td>
</tr>
<tr>
<td>policy condition tos</td>
</tr>
<tr>
<td>policy condition dscp</td>
</tr>
<tr>
<td>policy condition source mac</td>
</tr>
<tr>
<td>policy condition destination mac</td>
</tr>
<tr>
<td>policy condition source mac group</td>
</tr>
<tr>
<td>policy condition destination mac group</td>
</tr>
<tr>
<td>policy condition source vlan</td>
</tr>
<tr>
<td>policy condition inner source-vlan</td>
</tr>
<tr>
<td>policy condition destination vlan</td>
</tr>
<tr>
<td>policy condition 802.1p</td>
</tr>
<tr>
<td>policy condition inner 802.1p</td>
</tr>
<tr>
<td>policy condition source port</td>
</tr>
<tr>
<td>policy condition destination port</td>
</tr>
<tr>
<td>policy condition source port group</td>
</tr>
<tr>
<td>policy condition destination port group</td>
</tr>
<tr>
<td>policy condition vrf</td>
</tr>
<tr>
<td>policy condition fragments</td>
</tr>
<tr>
<td>policy condition app-mon-application-group</td>
</tr>
<tr>
<td>policy condition app-mon-application-name</td>
</tr>
<tr>
<td>policy condition appfp-group</td>
</tr>
</tbody>
</table>
Types of policies are generally determined by the kind of traffic they classify (policy conditions) and how the policy is enforced (policy actions). Commands used for particular types of policies are listed here. See the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about creating these types of policies and information about valid condition/action combinations.

<table>
<thead>
<tr>
<th>Action commands</th>
<th>policy action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policy action disposition</td>
</tr>
<tr>
<td></td>
<td>policy action shared</td>
</tr>
<tr>
<td></td>
<td>policy action priority</td>
</tr>
<tr>
<td></td>
<td>policy action maximum bandwidth</td>
</tr>
<tr>
<td></td>
<td>policy action maximum depth</td>
</tr>
<tr>
<td></td>
<td>policy action cir</td>
</tr>
<tr>
<td></td>
<td>policy action cpu priority</td>
</tr>
<tr>
<td></td>
<td>policy action tos</td>
</tr>
<tr>
<td></td>
<td>policy action 802.1p</td>
</tr>
<tr>
<td></td>
<td>policy action dscp</td>
</tr>
<tr>
<td></td>
<td>policy action map</td>
</tr>
<tr>
<td></td>
<td>policy action permanent gateway-ip</td>
</tr>
<tr>
<td></td>
<td>policy action permanent gateway-ipv6</td>
</tr>
<tr>
<td></td>
<td>policy action port-disable</td>
</tr>
<tr>
<td></td>
<td>policy action redirect port</td>
</tr>
<tr>
<td></td>
<td>policy action redirect linkagg</td>
</tr>
<tr>
<td></td>
<td>policy action no-cache</td>
</tr>
<tr>
<td></td>
<td>policy action mirror</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access Control Lists</th>
<th>policy condition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policy action disposition</td>
</tr>
<tr>
<td></td>
<td>policy rule</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic prioritization/shaping</th>
<th>policy action shared</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policy action priority</td>
</tr>
<tr>
<td></td>
<td>policy action maximum bandwidth</td>
</tr>
<tr>
<td></td>
<td>policy rule</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IEC 6185 traffic prioritization</th>
<th>iec message-type priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iec message-type flush</td>
</tr>
<tr>
<td></td>
<td>iec show</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>802.1p/ToS/DSCP tagging or mapping</th>
<th>policy condition tos</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policy condition dscp</td>
</tr>
<tr>
<td></td>
<td>policy condition 802.1p</td>
</tr>
<tr>
<td></td>
<td>policy action tos</td>
</tr>
<tr>
<td></td>
<td>policy action 802.1p</td>
</tr>
<tr>
<td></td>
<td>policy action dscp</td>
</tr>
<tr>
<td></td>
<td>policy action map</td>
</tr>
<tr>
<td></td>
<td>policy rule</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy based port mirroring</th>
<th>policy action mirror</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>VLAN Stacking</th>
<th>policy condition inner source-vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policy condition inner 802.1p</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VXLAN Snooping</th>
<th>policy condition vxlan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>policy condition vxlan inner source mac</td>
</tr>
<tr>
<td></td>
<td>policy condition vxlan inner source mac-group</td>
</tr>
<tr>
<td></td>
<td>policy condition vxlan inner source ip</td>
</tr>
<tr>
<td></td>
<td>policy condition vxlan inner source ipv6</td>
</tr>
<tr>
<td></td>
<td>policy condition vxlan inner ip-protocol</td>
</tr>
<tr>
<td></td>
<td>policy condition vxlan inner l4-port</td>
</tr>
<tr>
<td></td>
<td>policy condition vxlan vxlan-port</td>
</tr>
</tbody>
</table>
policy rule

Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

```
policy rule rule_name [enable | disable] [precedence precedence] [condition condition] [action action] [validity-period name] [save] [log [log-interval seconds]] [count {packets | bytes}] [trap] [default-list]
policy rule rule_name no {validity-period | save | log | trap | default-list}
no policy rule rule_name
```

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rule_name</code></td>
<td>The name of the policy rule, any alphanumeric string.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables the policy rule.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables the policy rule.</td>
</tr>
<tr>
<td><code>precedence</code></td>
<td>The precedence value in the range 0–65535. This value determines the order in which rules</td>
</tr>
<tr>
<td></td>
<td>are searched for a matching condition. A higher number indicates higher precedence. Typically</td>
</tr>
<tr>
<td></td>
<td>the range 30000–65535 is reserved for PolicyView.</td>
</tr>
<tr>
<td><code>condition</code></td>
<td>The condition name that is associated with this rule. Conditions are configured through the</td>
</tr>
<tr>
<td></td>
<td><code>policy condition</code> command.</td>
</tr>
<tr>
<td><code>action</code></td>
<td>The name of the action that is associated with this rule. Actions are configured through the</td>
</tr>
<tr>
<td></td>
<td><code>policy action</code> command.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>The name of a user-defined validity period that is associated with this rule. Validity</td>
</tr>
<tr>
<td></td>
<td>periods are configured through the <code>policy validity period</code> command.</td>
</tr>
<tr>
<td><code>save</code></td>
<td>Marks the policy rule so that it may be captured as part of the switch configuration.</td>
</tr>
<tr>
<td><code>log</code></td>
<td>Configures the switch to log messages about specific flows coming into the switch that match</td>
</tr>
<tr>
<td></td>
<td>this policy rule. This parameter is supported only on the OmniSwitch 6860, OmniSwitch 6865,</td>
</tr>
<tr>
<td></td>
<td>and OmniSwitch 6900.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>Configures how often to look for packets that match this policy rule when rule logging is</td>
</tr>
<tr>
<td></td>
<td>applied (in the range from 0–3600 seconds). A value of 0 specifies to log as often as possible.</td>
</tr>
<tr>
<td><code>packets</code></td>
<td>Counts the number of packets that match the rule. This parameter is supported only on the</td>
</tr>
<tr>
<td></td>
<td>OmniSwitch 6860(E), OmniSwitch 6865, and OmniSwitch 6900-X72.</td>
</tr>
<tr>
<td><code>bytes</code></td>
<td>Counts the number of bytes that match the rule. This parameter is supported only on the</td>
</tr>
<tr>
<td></td>
<td>OmniSwitch 6860(E), OmniSwitch 6865, and OmniSwitch 6900-X72.</td>
</tr>
<tr>
<td><code>trap</code></td>
<td>Enables or disables traps for the rule.</td>
</tr>
<tr>
<td><code>default-list</code></td>
<td>Adds the rule to the QoS default policy list.</td>
</tr>
</tbody>
</table>
Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>precedence</td>
<td>0</td>
</tr>
<tr>
<td>log</td>
<td>no</td>
</tr>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
<tr>
<td>packets</td>
<td>bytes</td>
</tr>
<tr>
<td>trap</td>
<td>enable</td>
</tr>
<tr>
<td>default-list</td>
<td>adds rule to the default list</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Any rule configured through this command is not active on the switch until the qos apply command is issued.

- A policy rule configured through the PolicyView application may not be edited in the CLI. You may, however, create a rule using the CLI with a higher precedence that will override a rule created through PolicyView.

- Use the no form of the command to remove the rule from the configuration or to remove parameters from a particular rule. The change will not take effect, however, until the qos apply command is issued.

- Only one validity period is associated with a policy rule. Each time this command is entered with a validity period name specified, the existing period name is overwritten with the new one.

- Software and hardware resources are allocated for rules associated with a validity period even if the validity period is not active. Pre-allocating the resources makes sure the rule can be enforced when the validity period becomes active.

- The save option marks the policy rule so that the rule will be captured in an ASCII text file (using the configuration snapshot command), saved to the working directory after the write memory command or copy running-config working command is entered, or saved after a reboot. Rules are saved by default. If no save is entered for the rule, the policy rule will not be written to the configuration. The save option should be disabled only if you want to use a policy rule temporarily.

- The default-list option adds the rule to the default policy list. Rules are added to this list by default when the rule is created. A rule can belong to multiple policy lists. As a result, the rule remains a
member of the default list even when it is subsequently assigned to additional lists. Consider the following recommendations regarding the default policy list:

- If the rule is going to belong to a QoS policy list for a Universal Network Profile (UNP), use the `no default-list` option when creating the rule. Doing so will give the rule precedence over default list rules when the policy list is applied to UNP device traffic.

- Note that each time a rule is assigned to a policy list, an instance of that rule is created and each instance is allocated system resources. Use the `no default-list` option with this command to exclude the rule from the default policy list.

- When creating a policy rule with a destination port condition on an OmniSwitch 9900, specify the `no default-list` option to ensure that this type of condition is supported on the OmniSwitch 9900. See the `policy condition destination port` command.

- The `log` option is useful for determining the source of attacks on the switch firewall.

- The `log` option is not supported for service domain traffic.

- If traps are enabled for the rule, a trap is only sent when a port disable action or UserPort shutdown operation is triggered.

- If the `configuration snapshot` command is entered after the `policy rule` command is configured, the resulting ASCII file will include the following additional syntax for the `policy rule` command:

  ```
  from {cli | ldap | blt}
  ```

  This syntax indicates how the rule was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in rule, this setting is not configurable.

**Examples**

- `> policy rule rule2 condition c2 action a2`
- `> policy rule rule3 condition c3 action a3 no default-list`
- `> policy rule rule2 precedence 65535`
- `> policy rule rule2 validity-period vp01`
- `> policy rule rule2 no precedence`
- `> policy rule rule2 no validity-period`
- `> policy rule rule3 no default-list`
- `> no policy rule rule2`

**Release History**

Release 7.1.1; command was introduced.
Release 8.8R2; `trap` keyword deprecated.
Related Commands

**iec message-type priority**
- Configures a validity period that specifies days, times, and/or months during which an associated policy rule is in effect.

**policy condition**
- Configures condition parameters.

**policy action**
- Configures action parameters.

**qos apply**
- Applies configured QoS and policy settings to the current configuration.

**show policy rule**
- Displays information for policy rules configured on the switch.

**show active policy rule**
- Displays only those policy rules that are currently being enforced on the switch.

MIB Objects

- `alaQoSRuleTable`
  - `alaQoSRuleName`
  - `alaQoSRuleEnabled`
  - `alaQoSRuleSource`
  - `alaQoSRulePrecedence`
  - `alaQoSRuleCondition`
  - `alaQoSRuleAction`
  - `alaQoSRuleSave`
  - `alaQoSRuleLog`
  - `alaQoSRuleCountType`
  - `alaQoSRulePacketCount`
  - `alaQoSRuleByteCount`
  - `alaQosRuleDefaultList`

- `alaQoSAppliedRuleTable`
  - `alaQoSAppliedRuleName`
  - `alaQoSAppliedRuleEnabled`
  - `alaQoSAppliedRuleSource`
  - `alaQoSAppliedRulePrecedence`
  - `alaQoSAppliedRuleCondition`
  - `alaQoSAppliedRuleAction`
  - `alaQoSAppliedRuleSave`
  - `alaQoSAppliedRuleLog`
  - `alaQoSAppliedCountType`
  - `alaQoSAppliedPacketCount`
  - `alaQoSAppliedByteCount`
  - `alaQosAppliedDefaultList`
**iec message-type priority**

Configures a QoS priority for the specified IEC 61850 message type. This command runs a python script that programs QoS rules that will apply traffic prioritization to IEC 61850 message packets.

**Syntax Definitions**

- **message**
  The message type for which a QoS rule is configured. Specify one of the supported IEC 61850 message types: goose, gse, sv, ptp, snmp, mms, all.

- **priority string**
  Sets the priority level. The priority string value must be set to one of the following:
  - “high” (maps to QoS priority queue 7)
  - “medium” (maps to QoS priority queue 4)
  - “low” (maps to QoS priority queue 1)
  - “default” (sets the priority to the default value for the message type)

**Defaults**

By default, the priority for all the supported IEC 61850 message type is set to default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- To set the priority for all message types at once, specify “all” as the message type value.
- A message type can be configured with only one priority.
- Use the “default” option to restore the default priority as shown in the table:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Default Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOOSE</td>
<td>High</td>
</tr>
<tr>
<td>GSE</td>
<td>Medium</td>
</tr>
<tr>
<td>SV</td>
<td>High</td>
</tr>
<tr>
<td>MMS</td>
<td>Low</td>
</tr>
<tr>
<td>SNTP</td>
<td>Medium</td>
</tr>
<tr>
<td>PTP</td>
<td>Medium</td>
</tr>
</tbody>
</table>
The QoS policy condition, action, and rule names that are used to prioritize IEC 61759 traffic are predefined. The following reserved names must not be used for user policy configuration:
Use the `iec message-type flush` CLI command to remove the prioritization for message type.

**Examples**

- `-> iec message-type goose priority high`
- `-> iec message-type gse priority low`
- `-> iec message-type mms priority medium`
- `-> iec message-type all priority high`

**Release History**

Release 8.7 R1; command was introduced.

**Related Commands**

- `iec message-type flush` Removes the rule applied for the IEC 61850 message priority.
- `iec show` Displays the priority configured for the IEC 61850 message types.

**MIB Objects**

```
N/A
```
**iec message-type flush**

Removes the rule applied for the IEC 61850 message priority.

**Syntax Definitions**

`message` The message type for which rule must be flushed. Specify one of the supported IEC 61850 message types: goose, gse, sv, ptp, sntp, mms, all.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command runs a python script that programs the QoS rules for traffic prioritization.
- The “all” option flushes the priority rule for all the message types at once.

**Examples**

- `-> iec message-type goose flush`
- `-> iec message-type gse flush`
- `-> iec message-type mms flush`
- `-> iec message-type all flush`

**Release History**

Release 8.7 R1; command was introduced.

**Related Commands**

- `iec message-type priority` Configures IEC 61850 message priority.
- `iec show` Displays the priority configured for the IEC 61850 message types.

**MIB Objects**

N/A
**iec show**

Displays the priority configured for the IEC 61850 message types.

```plaintext
-> iec show
Message Type   Priority
---------------+------------
goose          high
sntp           low
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output displays only the configured message types.

**Examples**

```plaintext
-> iec show
Message Type   Priority
---------------+------------
goose          high
sntp           low
```

**Release History**

Release 8.7 R1; command was introduced.

**Related Commands**

- `iec message-type priority` Configures IEC 61850 message priority.

**MIB Objects**

N/A
policy validity-period

Configures a validity period that specifies the days and times in which a policy rule is in effect.

\texttt{policy validity-period name [days \texttt{days}] [months \texttt{months}] [hours \texttt{hh:mm to hh:mm}] [interval mm:dd:yy \texttt{hh:mm to mm:dd:yy hh:mm}]}

\texttt{policy validity-period name no \{hours | interval\}}

\texttt{no policy validity-period name}

\subsection*{Syntax Definitions}

\begin{itemize}
  \item \texttt{name} The name of the validity period (up to 31 alphanumeric characters).
  \item \texttt{days} The day(s) of the week this validity period is active. Enter the actual day of the week (e.g., \texttt{monday}, \texttt{tuesday}, \texttt{wednesday}, etc.).
  \item \texttt{months} The month(s) in which the validity period is active. Enter the actual month (e.g., \texttt{january}, \texttt{february}, \texttt{march}, etc.).
  \item \texttt{hh:mm} The time of day, specified in hours and minutes, the validity period starts and the time of day the validity period ends (e.g., 10:30 to 11:30).
  \item \texttt{mm:dd:yy hh:mm} An interval of time during which a rule is in effect. Specify a start and end to the interval period by entering a beginning date and time followed by an end date and time (e.g., 11:01:17 12:01 to 11:02:17 12:01).
\end{itemize}

\subsection*{Defaults}

By default, no validity period is in effect for a policy rule.

\begin{table}[h]
\centering
\begin{tabular}{l l}
\textbf{Parameter} & \textbf{Default} \\
\hline
\texttt{days} & no restriction \\
\texttt{months} & no restriction \\
\texttt{hh:mm} & no specific time \\
\texttt{mm:dd:yyyy hh:mm} & no interval \\
\end{tabular}
\end{table}

\subsection*{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|c|c|c|c|c|c|}
\hline
\hline
Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes \\
\hline
\end{tabular}
\end{table}
**Usage Guidelines**

- Use the **no** form of the command to remove a validity period from the configuration, or to remove parameters from a particular validity period. Note that at least one parameter must be associated with a validity period.

- Any combination of days, months, hours, and interval parameters is allowed. The validity period is only in effect when all specified parameters are true.

- Use the **policy rule** command to associate a validity period with a rule.

- Software and hardware resources are allocated for rules associated with a validity period even if the validity period is not active. Pre-allocating the resources makes sure the rule can be enforced when the validity period becomes active.

- If the **configuration snapshot** command is entered after the **policy validity-period** command is configured, the resulting ASCII file will include the following additional syntax for the **policy validity-period** command:

  from {cli | ldap | blt}

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

**Examples**

```bash
-> policy validity-period vp01 days tuesday thursday months january february
-> policy validity-period vp01 hours 13:00 to 19:00
-> policy validity-period vp02 interval 01/01/05 12:01 to 02/01/05 11:59
-> policy validity-period vp01 no days thursday
-> no policy-validity period vp02
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **policy rule**: Configures a policy rule on the switch and optionally associates that rule with a validity period.

- **show policy validity period**: Displays information about policy validity periods.
MIB Objects

alaQoSValidityPeriodTable
alaQoSValidityPeriodName
alaQoSValidityPeriodSource
alaQoSValidityPeriodDays
alaQoSValidityPeriodDaysStatus
alaQoSValidityPeriodMonths
alaQoSValidityPeriodMonthsStatus
alaQoSValidityPeriodHour
alaQoSValidityPeriodHourStatus
alaQoSValidityPeriodEndHour
alaQoSValidityPeriodInterval
alaQoSValidityPeriodIntervalStatus
alaQoSValidityPeriodEndInterval

alaQoSAppliedValidityPeriodTable
alaQoSAppliedValidityPeriodName
alaQoSAppliedValidityPeriodSource
alaQoSAppliedValidityPeriodDays
alaQoSAppliedValidityPeriodDaysStatus
alaQoSAppliedValidityPeriodMonths
alaQoSAppliedValidityPeriodMonthsStatus
alaQoSAppliedValidityPeriodHour
alaQoSAppliedValidityPeriodHourStatus
alaQoSAppliedValidityPeriodEndHour
alaQoSAppliedValidityPeriodInterval
alaQoSAppliedValidityPeriodIntervalStatus
alaQoSAppliedValidityPeriodEndInterval
**policy list**

Configures a QoS policy list. There are four types of lists available: a Universal Network Profile (UNP) policy list, an egress policy list, an Application Fingerprinting policy list, and a default policy list.

```
policy list list_name type {unp | egress | appfp | empacl} [enable | disable]
nopolicy list list_name
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>list_name</code></td>
<td>The name to assign to the policy list. Note that the list name is case sensitive.</td>
</tr>
<tr>
<td><code>unp</code></td>
<td>Applies the list of policy rules to traffic classified into the User Network Profile to which the list is assigned.</td>
</tr>
<tr>
<td><code>egress</code></td>
<td>Applies the list of policy rules to traffic egressing on switch ports. <em>This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560, and OmniSwitch 6570M.</em></td>
</tr>
<tr>
<td><code>appfp</code></td>
<td>Applies the list of policy rules to an Application Fingerprinting interface. <em>This parameter is supported only on the OmniSwitch 6900.</em></td>
</tr>
<tr>
<td><code>empacl</code></td>
<td><em>This parameter is not supported.</em></td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables the policy list.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables the policy list.</td>
</tr>
</tbody>
</table>

### Defaults

A default policy list is available when the switch boots up; all policy rules belong to this list unless otherwise specified (see the `policy list rules` and `policy rule` commands for more information).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td><code>enable</code></td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove a policy list from the configuration.
- Once a policy list is created, use the `policy list rules` command to add rules to the list.
• Any policy list configured through this command is not active on the switch until the `qos apply` command is issued.

• If the `configuration snapshot` command is entered after the `policy list` command is configured, the resulting ASCII file will include the following additional syntax for the `policy list` command:

`from {cli | ldap | blt}`

This syntax indicates how the list was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in object, this setting is not configurable.

**Examples**

```- policy list unp1 type unp
- policy list unp1 disable
- policy list unp1 enable
- no policy list unp1```

**Release History**

Release 7.2.1; command was introduced.
Release 8.4.1; `egress` parameter added.

**Related Commands**

- `policy list rules` Assigns QoS policy rules to a QoS policy list.
- `policy rule` Configures a policy rule on the switch and optionally associates that rule with a validity period.
- `show policy rule` Displays information for policy rules configured on the switch.
- `show active policy list` Displays only those policy lists that are currently being enforced on the switch.
- `show policy list` Displays information for policy lists configured on the switch.

**MIB Objects**

alaQoSRuleGroupsTable
  - `alaQoSRuleDefaultList`  
  - `alaQoSRuleGroupsName`  
  - `alaQoSRuleGroupsSource`  
  - `alaQoSRuleGroupsType`  
  - `alaQoSRuleGroupsEnabled`  
  - `alaQoSRuleGroupsStatus`  

alaQosAppliedRuleGroupsTable
  - `alaQosAppliedRuleGroupsName`  
  - `alaQosAppliedRuleGroupsSource`  
  - `alaQosAppliedGroupsType`  
  - `alaQosAppliedGroupsEnabled`  
  - `alaQosAppliedRuleGroupsStatus`
policy list rules

Assigns existing QoS policy rules to the specified QoS policy list.

`policy list list_name rules rule_name [rule_name2...]`

`policy list list_name no rules rule_name [rule_name2...]`

**Syntax Definitions**

- **list_name**
  The name of an existing QoS policy list. Note that the list name is case sensitive.

- **rule_name**
  The name of an existing QoS policy rule to include in the policy list.

- **rule_name2**
  Optional. The name of another QoS policy rule to include in the policy list. Separate each rule name specified with a space.

**Defaults**

A default policy list is available when the switch boots up. This list has no name and is not configurable. All QoS policy rules are assigned to the default list unless the `no default-list` option of the `policy rule` command is used.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>6900</th>
<th>X48C4E/V48C8/</th>
<th>9900</th>
<th>X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a policy rule from an existing list.

- The QoS policy list and rule names specified with this command must already exist in the switch configuration.

- A rule may belong to a Universal Network Profile (UNP) list, the default list, and an egress policy list at the same time. By default, a rule is assigned to a default policy list when the rule is created. If the rule is subsequently assigned to another policy list, it still remains associated with the default list.

- If a rule is a member of multiple policy lists but one or more of these lists are disabled, the rule is still active in those lists that are enabled.

- If the QoS status of a policy rule is disabled, then the rule is disabled for all lists even if a list to which the policy rule belongs is enabled.

- If a policy rule is going to be assigned to a UNP policy list, make sure the rule was created using the `no default-list` option of the `policy rule` command. This will ensure that the rule will take precedence over other default list rules when the UNP policy list is applied to device traffic.
A QoS policy list that is assigned to an Application Fingerprinting interface must contain policy rules with the `appfp-group` condition.

- Only those rules that are assigned to an egress policy list are applied to egress traffic. When configuring egress policy lists, consider the following:
  - Egress policy lists are not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 and OmniSwitch 6570M.
  - Only one egress policy list per switch is supported, to which IPv4 and IPv6 rules can be added.
  - Applying egress policy lists to SPB or VXLAN SAP ports is not supported.
  - Only the following policy conditions and actions are supported when creating rules for an egress policy list:

<table>
<thead>
<tr>
<th>policy conditions</th>
<th>policy actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination port</td>
<td>Disposition (drop/accept)</td>
</tr>
<tr>
<td>Destination VLAN</td>
<td></td>
</tr>
<tr>
<td>Source IPv4 address</td>
<td></td>
</tr>
<tr>
<td>Source IPv6 address</td>
<td></td>
</tr>
<tr>
<td>IPv6 (qualifier for traffic types)</td>
<td></td>
</tr>
</tbody>
</table>

- On an OmniSwitch 9900, a destination port condition is supported only when the condition is part of a policy rule that was configured using the `no default-list` option (for example, `policy rule r1 condition c1 action a1 no default-list`). See the `policy condition destination port` command.

- Using policy lists that contain rules with a source port condition are not supported when applied to 10G ports on an OmniSwitch 6560 and OmniSwitch 6570M.

- On the OmniSwitch 6360 and OmniSwitch 6465, policy rules containing the following conditions are not supported in a UNP policy list:
  - Source port group
  - Source IPv6 address
  - IPv6 flow label
  - Source MAC/MAC group
  - Destination MAC/MAC group
  - Ethertype for IPV6

- On the OmniSwitch 6360, OmniSwitch 6560, OmniSwitch 6570M and OmniSwitch 9900, only policy rules with the following conditions can be assigned to a UNP policy list:
  - Destination MAC
  - EtherType
  - Source VLAN
  - SIP
  - DIP / DIPv6
  - Layer 4 Protocol
  - Layer 4 source port
  - Layer 4 destination port
  - Source port

- Any policy list configured through this command is not active on the switch until the `qos apply` command is issued.
Examples

-> policy list unp1 rules r1 r2 r3
-> policy list unp1 no rules r2

Release History

Release 7.2.1; command was introduced.

Related Commands

- policy list: Configures a QoS policy list.
- policy rule: Configures a policy rule on the switch and optionally associates that rule with a validity period.
- show policy rule: Displays information for policy rules configured on the switch.
- show active policy list: Displays only those policy lists that are currently being enforced on the switch.
- show policy list: Displays information for policy lists configured on the switch.

MIB Objects

alaQoSRuleGroupsTable
  alaQoSRuleDefaultList
  alaQoSRuleGroupsName
  alaQoSRuleGroupsSource
  alaQoSRuleGroupsType
  alaQoSRuleGroupsEnabled
  alaQoSRuleGroupsStatus

alaQosAppliedRuleGroupsTable
  alaQosAppliedRuleGroupsName
  alaQosAppliedRuleGroupsSource
  alaQosAppliedGroupsType
  alaQosAppliedGroupsEnabled
  alaQosAppliedRuleGroupsStatus
policy network group

Configures a network group name and its associated IP addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the network group.

```
policy network group net_group ip_address [mask net_mask] [ip_address2 [mask net_mask2]...]
no policy network group net_group
policy network group net_group no ip_address [mask netmask] [ip_address2 [mask net_mask2]...]
```

Syntax Definitions

- **net_group**: The name of the network group (up to 31 alphanumeric characters).
- **ip_address**: An IPv4 or IPv6 address included in the network group.
- **net_mask**: The mask for the IPv4 or IPv6 address. If no mask is entered, the address is assumed to be a host address.
- **ip_address2**: Optional. Another IPv4 or IPv6 address to be included in the network group. Multiple IP addresses may be configured for a network group. Separate each address/mask combination with a space.
- **net_mask2**: Optional mask for the IPv4 or IPv6 address. If no mask is entered, the natural mask for the address will be used.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use this command to configure a group of IP addresses to which you want to apply QoS rules. Rather than create a condition for each IP address, group the addresses together. Use the policy condition command to associate a condition with the network group.

- Use the no form of the command to remove a network group from the configuration, or to remove an IP address from a network group.
If the configuration snapshot command is entered after the policy network group command is configured, the resulting ASCII file will include the following additional syntax for the policy network group command:

```
from {cli | ldap | blt}
```

This syntax indicates how the network group was created. The cli and ldap options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The blt option indicates a built-in network group, this setting is not configurable.

**Examples**

```
-> policy network group webgroup1 10.10.12.5 10.50.3.1
-> policy network group webgroup1 no 10.10.12.5
-> no policy network group webgroup1

-> policy network group webgroup2 no 2002:c633:6489::35
-> no policy network group webgroup2
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **policy condition**: Configures a policy condition. A network group may be configured as part of a policy condition.
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **show policy network group**: Displays information for policy network groups.

**MIB Objects**

- `alaQoSNetworkGroupsTable`
  - `alaQoSNetworkGroupsName`
  - `alaQoSNetworkGroupsSource`
- `alaQoSAppliedNetworkGroupsTable`
  - `alaQoSAppliedNetworkGroupsName`
  - `alaQoSAppliedNetworkGroupsSource`
- `alaQoSNetworkGroupTable`
  - `alaQoSNetworkGroupIpAddr`
  - `alaQoSNetworkGroupsIpMask`
- `alaQoSAppliedNetworkGroupTable`
  - `alaQoSAppliedNetworkGroupIpAddr`
  - `alaQoSAppliedNetworkGroupsIpMask`
**policy service group**

Configures a service group and its associated services. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the service group.

```
policy service group service_group service_name1 [service_name2...]
no policy service group service_group
policy service group service_group no service_name1 [service_name2...]
```

### Syntax Definitions

- **service_group**
  - The name of the service group (up to 31 alphanumeric characters).

- **service_name1**
  - The service name is configured through the `policy service` command and includes information about protocol, source port, and destination port.

- **service_name2...**
  - Optional. Additional service names may be configured for a service group. Separate each service name with a space.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use this command to configure a group of services to which you want to apply QoS rules. Rather than create a condition for each service, group services together. Use the `policy condition` command to associate a condition with the service group.

- Use the `no` form of the command to remove a service group from the configuration, or to remove a service from a service group.

- To drop packets destined to specific TCP and UDP ports, create port services for the traffic that you want dropped and add these services to a service group. Then create a condition for this service group and a source port group, which can then be used in a deny rule. Refer to the *OmniSwitch AOS Release 8 Network Configuration Guide* for more information about ACL security enhancements.
If the configuration snapshot command is entered after the policy service group command is configured, the resulting ASCII file will include the following additional syntax for the policy service group command:

from {cli | ldap | blt}

This syntax indicates how the service group was created. The cli and ldap options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The blt option indicates a built-in service group, this setting is not configurable.

Examples

-> policy service group servgroup2 telnet ftp
-> policy service group servgroup2 no telnet
-> no policy service group servgroup2

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply  Applies configured QoS and policy settings to the current configuration.
policy service  Configures a service that may be used as part of a policy service group.
policy condition  Configures a policy condition. A network group may be configured as part of a policy condition.
show policy service group  Displays information for policy service groups.

MIB Objects

alaQoSServiceGroupsTable
   alaQoSServiceGroupsName
   alaQoSServiceGroupsSource
alaQoSAppliedServiceGroupsTable
   alaQoSAppliedServiceGroupsName
   alaQoSAppliedServiceGroupsSource
alaQoSServiceGroupTable
   alaQoSServiceGroupServiceName
alaQoSAppliedServiceGroupTable
   alaQoSAppliedServiceGroupServiceName
**policy mac group**

Configures a MAC group and its associated MAC addresses. The group may be used as part of a policy condition. The action associated with any policy using the condition will be applied to all members of the MAC group.

```plaintext
policy mac group mac_group mac_address [mask mac_mask] [mac_address2 [mask mac_mask2]...]
no policy mac group mac_group
policy mac group mac_group no mac_address [mask mac_mask] [mac_address2 [mask mac_mask2]...]
```

---

**Syntax Definitions**

- `mac_group` The name of the MAC group (up to 31 alphanumeric characters).
- `mac_address` The MAC address associated with the group (for example, 00:20:da:05:f6:23).
- `mac_mask` The mask of the MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.
- `mac_address2` Optional. Additional MAC addresses may be configured for a MAC group. Separate each address with a space.
- `mac_mask2` The mask of an additional MAC address, used to identify which bytes in the MAC address are significant when comparing the MAC address in the received frame with the MAC address in the policy condition. If no mask is specified, the switch automatically uses ff:ff:ff:ff:ff:ff.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use this command to configure a group of source or destination MAC addresses to which you want to apply QoS rules. Rather than create a condition for each MAC address, group MAC addresses together. Use the `policy condition` command to associate a condition with the MAC group.
- Use the `no` form of the command to remove a MAC group from the configuration, or to remove a MAC address from a MAC group.
- The MAC group name “alaPhones” is a reserved group name used to identify the MAC addresses of IP phones. See the `qos phones` command for more information.

- If the `configuration snapshot` command is entered after the `policy map group` command is configured, the resulting ASCII file will include the following additional syntax for the `policy map group` command:

  ```
  from {cli | ldap | blt}
  ```

  This syntax indicates how the map group was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in object, this setting is not configurable.

**Examples**

```bash
-> policy mac group mac_group1 00:20:da:05:f6:23 00:20:da:05:f6:24
-> no policy mac group mac_group1
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `policy condition`: Configures a policy condition. A MAC group may be configured as part of a policy condition.
- `qos apply`: Applies configured QoS and policy settings to the current configuration.
- `show policy mac group`: Displays information about policy MAC groups.

**MIB Objects**

- `alaQoSMACGroupsTable`
  - `alaQoSMACGroupsName`
  - `alaQoSMACGroupsSource`
- `alaQoSAppliedMACGroupsTable`
  - `alaQoSAppliedMACGroupsName`
  - `alaQoSAppliedMACGroupsSource`
- `alaQoSMACGroupTable`
  - `alaQoSMACGroupMacAddr`
  - `alaQoSMACGroupMacMask`
- `alaQoSAppliedMACGroupTable`
  - `alaQoSAppliedMACGroupMacAddr`
  - `alaQoSAppliedMACGroupMacMask`
**policy port group**

Configures a port group and its associated slot and port numbers. A port group may be attached to a policy condition. The action associated with that policy will be applied to all members of the port group.

```
policy port group group_name {chassis//slot/port[-port2] | agg_id[-agg_id2]} [chassis//slot/port[-port2] | agg_id[-agg_id2]]
```

```
no policy port group group_name
```

```
policy port group group_name no {chassis//slot/port[-port2] | agg_id[-agg_id2]} [chassis//slot/port[-port2] | agg_id[-agg_id2]]
```

**Syntax Definitions**

- **group_name**: The name of the port group (up to 31 alphanumeric characters).
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port (or port range) to be included in the group. At least one slot/port combination must be specified. Additional combinations may be included in the group; each combination should be separated by a space.
- **agg_id[-agg_id2]**: A link aggregate ID to be included in the group. Use a hyphen to specify a range of IDs (10-15). Additional combinations may be included in the group; each combination should be separated by a space.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to configure a group of ports or link aggregates to which you want to apply QoS rules. Rather than create a condition for each port, group ports together. Use the **policy condition** command to associate a condition with the port group.

- Configuring ports and link aggregates in the same port group is allowed.

- Adding link aggregate member ports to a QoS port group is not recommended; doing so may cause undesired results when the port group is used in a QoS policy, particularly if only a subset of member ports is added to the port group.
• Use the `no` form of the command to remove a port group from the configuration, or to remove a slot/port from a port group.

• If a range of ports is specified using the syntax `chassis/slot/port-port2` (that is, 1/2/1-8), a single port within that range cannot be removed on its own. The entire range must be deleted as it was entered.

• If a range of link aggregates is specified using the syntax `agg_id1-agg_id2` (that is, 10-15), a single aggregate within that range cannot be removed on its own. The entire range must be deleted as it was entered.

• When a port group is used as part of a policy rule and a policy action specifies a maximum bandwidth, each interface in the port group will be allowed the maximum bandwidth.

• To prevent IP source address spoofing, add ports to the port group called `UserPorts`. `UserPorts` name is case sensitive. This port group does not need to be used in a condition or rule to be effected on flows and applies to both VLAN domain and service domain for both bridged and routed traffic. Ports added to the `UserPorts` group will block spoofed traffic while still allowing normal traffic on the port. Refer to the `OmniSwitch AOS Release 8 Network Configuration Guide` for more information about ACL security enhancements.

• Anti-spoofing on service is supported only on SPB SAP ports and is supported on OmniSwitch 6860N, and OmniSwitch 6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2 where inline routing is supported.

• Link aggregate addition is not supported in QoS `UserPorts` port group.

• Use the `qos user-port` command to configure the option to filter or administratively disable a port when a specific type of traffic (Spoof, RIP, BPDU, OSPF, and/or BGP) is received on a port that is a member of the pre-defined `UserPorts` group.

• If the `configuration snapshot` command is entered after the `policy port group` command is configured, the resulting ASCII file will include the following additional syntax for the `policy port group` command:

```plaintext
from {cli | ldap | blt}
```

This syntax indicates how the port group was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in object, this setting is not configurable.

### Examples

```plaintext
-> policy port group port_group4 3/1/1-2 4/3/1 5/4/1
-> policy port group port_group4 no 3/1/1-2
-> policy port group UserPorts 4/1/1-8 5/1/1-8
```

### Release History

Release 7.1.1; command was introduced.
Release 8.3.1; `agg_id` parameter added.
Related Commands

**policy condition**
Configures a policy condition. A port group may be configured as part of a policy condition.

**qos apply**
Applies configured QoS and policy settings to the current configuration.

**policy action maximum bandwidth**
Configures a maximum bandwidth value for a policy action.

**show policy port group**
Displays information about policy port groups.

MIB Objects

alaQoSPortGroupsTable
- alaQoSPortGroupsName
- alaQoSPortGroupSlot
- alaQoSPortGroupPort
- alaQoSPortGroupPortEnd

alaQoSAppliedPortGroupsTable
- alaQoSAppliedPortGroupsName
- alaQoSAppliedPortGroupSlot
- alaQoSAppliedPortGroupPort
- alaQoSAppliedPortGroupPortEnd
**policy map group**

Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values. A map group may be referenced in a policy action with the `map` keyword.

```
policy map group map_group {value1:value2...}
no policy map group map_group
policy map group no {value1:value2...}
```

**Syntax Definitions**

- `map_group`  
  The name of the map group (up to 31 alphanumeric characters).

- `value1`  
  The 802.1p, ToS, or DSCP value to be mapped to another value. May be a value or a range of values (for example, 1-2).

- `value2...`  
  The 802.1p, ToS, or DSCP value to be used in place of `value1`. Additional mapping pairs may be included.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a mapping pair or to remove the map group entirely.

- The map group may contain more than one mapping pair.

- If the `configuration snapshot` command is entered after the `policy map group` command is configured, the resulting ASCII file will include the following additional syntax for the `policy map group` command:

  ```
  from {cli | ldap | blt}
  ```

  This syntax indicates how the map group was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in object, this setting is not configurable.
Examples
- `policy map group tosGroup 1-4:3 5-6:5 7:6`
- `policy map group tosGroup no 7:6`
- `no policy map group tosGroup`

Release History
Release 7.1.1; command was introduced.

Related Commands

```
policy action map
```
Configures a mapping group for a policy action.

MIB Objects

```
alaQoSMapGroupsTable
  alaQoSMapGroupsName
  alaQoSMapGroupsSource
alaQoSAppliedMapGroupsTable
  alaQoSAppliedMapGroupsName
  alaQoSAppliedMapGroupsSource
alaQoSMapGroupTable
  alaQoSMapGroupKey
  alaQoSMapGroupKeyEnd
  alaQoSMapGroupValue
alaQoSAppliedMapGroupTable
  alaQoSAppliedMapGroupKey
  alaQoSAppliedMapGroupKeyEnd
  alaQoSAppliedMapGroupValue
```
**policy service**

Configures a service that may be used as part of a policy service group or included as part of a policy condition. A service is a source and/or destination TCP or UDP port or port range.

This overview section describes the base command. *At least one option must be configured with the base command.* Some options may be used in combination; some options are shortcuts for keyword combinations (see the Usage Guidelines). Options are described as separate commands. See the command descriptions and usage guidelines for valid combinations.

Use the **no** form for keywords to remove a parameter from a service.

```
policy service service_name
  [protocol protocol]
  [source ip-port port[-port]]
  [destination ip-port port[-port]]
  [source tcp-port port[-port]]
  [destination tcp-port port[-port]]
  [source udp-port port[-port]]
  [destination udp-port port[-port]]

no policy service service_name
```

**Syntax Definitions**

- `service_name`: The name of the service (up to 31 alphanumeric characters).
- `protocol`: The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported. This value must be specified for `source ip-port` or `destination ip-port`; it cannot be specified for `source tcp-port`, `destination tcp-port`, `source udp-port`, or `destination udp-port`.
- `port`: The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. Specify a range of ports using a hyphen (for example, 22-23).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the `no` form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.

- The command options offer alternate ways of configuring TCP or UDP ports for a service. Note that port types (TCP or UDP) cannot be mixed in the same service. The following table shows how the keywords are used:

<table>
<thead>
<tr>
<th>To configure:</th>
<th>Use keywords:</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP or UDP ports for a service</td>
<td>protocol source ip-port destination ip-port</td>
<td>The protocol must be specified with at least one source or destination port.</td>
</tr>
<tr>
<td>TCP ports for a service</td>
<td>source tcp-port destination tcp-port</td>
<td>Keywords may be used in combination.</td>
</tr>
<tr>
<td>UDP ports for a service</td>
<td>source udp-port destination udp-port</td>
<td>Keywords may be used in combination.</td>
</tr>
</tbody>
</table>

- If the `configuration snapshot` command is entered after the `policy service` command is configured, the resulting ASCII file will include the following additional syntax for the `policy service` command:

  `from {cli | ldap | blt}`

  This syntax indicates how the service was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in object, this setting is not configurable.

Examples

The following two commands show two different ways of configuring the same service:

  -> policy service telnet2 protocol 6 destination ip-port 23
  -> policy service telnet3 destination tcp-port 23

Release History

Release 7.1.1; command was introduced.

Related Commands

- `policy service group`: Configures a policy service group, which is made up of policy services.
- `policy condition`: Creates a policy condition.
- `qos apply`: Applies configured QoS and policy settings to the current configuration.
- `show policy service`: Displays information about policy services configured on the switch.
**MIB Objects**

alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceIpProtocol
   alaQoSServiceSourceIpPort
   alaQoSServiceSourceIpPortEnd
   alaQoSServiceDestinationIpPort
   alaQoSServiceDestinationIpPortEnd
   alaQoSServiceSourceTcpPort
   alaQoSServiceSourceTcpPortEnd
   alaQoSServiceDestinationTcpPort
   alaQoSServiceDestinationTcpPortEnd
   alaQoSServiceSourceUdpPort
   alaQoSServiceSourceUdpPortEnd
   alaQoSServiceDestinationUdpPort
   alaQoSServiceDestinationUdpPortEnd

alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedServiceIpProtocol
   alaQoSAppliedSourceIpPort
   alaQoSAppliedSourceIpPortEnd
   alaQoSAppliedServiceDestinationIpPort
   alaQoSAppliedServiceDestinationIpPortEnd
   alaQoSAppliedSourceTcpPort
   alaQoSAppliedSourceTcpPortEnd
   alaQoSAppliedServiceDestinationTcpPort
   alaQoSAppliedServiceDestinationTcpPortEnd
   alaQoSAppliedSourceUdpPort
   alaQoSAppliedSourceUdpPortEnd
   alaQoSAppliedServiceDestinationUdpPort
   alaQoSAppliedServiceDestinationUdpPortEnd
policy service protocol

Configures a service with a protocol and IP port or port range that may be used as part of a policy service group or included as part of a policy condition.

```
policy service service_name protocol protocol {[source ip-port port[-port]] [destination ip-port port[-port]]}
```

```
no policy service service_name
```

```
policy service service_name no {source ip-port | destination ip-port}
```

Syntax Definitions

- **service_name**: The name of the service (up to 31 alphanumeric characters).
- **protocol**: The protocol associated with the service. The range of values is 0–255. Currently a value of 6 (for TCP) or 17 (for UDP) is supported.
- **port**: The well-known port number (or port range) for the desired service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, 22-23).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of the command to remove a service from the configuration or to remove parameters from a particular service. (A protocol value cannot be removed from a service.)

- Shortcut commands for the **policy service protocol** command include the following: **policy service source tcp-port**, **policy service destination tcp-port**, **policy service source udp-port**, and **policy service destination udp-port**.

- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

```
from {cli | ldap | blt}
```

This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.
Examples

-> policy service telnet2 protocol 6 destination ip-port 23 source ip-port 22
-> policy service telnet2 no source ip-port

Release History

Release 7.1.1; command was introduced.

Related Commands

- `policy service group` Configures a policy service group, which is made up of policy services.
- `policy condition` Creates a policy condition.
- `qos apply` Applies configured QoS and policy settings to the current configuration.
- `show policy service` Displays information about policy services configured on the switch.

MIB Objects

- `alaQoSServiceTable`  
  - `alaQoSServiceName`  
  - `alaQoSServiceSource`  
  - `alaQoSServiceIpProtocol`  
  - `alaQoSServiceSourceIpPort`  
  - `alaQoSServiceSourceIpPortEnd`  
  - `alaQoSServiceDestinationIpPort`  
  - `alaQoSServiceDestinationIpPortEnd`

- `alaQoSAppliedServiceTable`  
  - `alaQoSAppliedServiceName`  
  - `alaQoSAppliedServiceSource`  
  - `alaQoSAppliedServiceIpProtocol`  
  - `alaQoSAppliedSourceIpPort`  
  - `alaQoSAppliedSourceIpPortEnd`  
  - `alaQoSAppliedServiceDestinationIpPort`  
  - `alaQoSAppliedServiceDestinationIpPortEnd`
policy service source tcp-port

Configures a service with a source TCP port or port range that may be used as part of a policy service group or included as part of a policy condition.

\textbf{policy service service\_name source tcp-port port[-port]}\textbf{no policy service service\_name}

\textbf{policy service service\_name no source tcp-port}

\underline{Syntax Definitions}

\begin{itemize}
  \item \textit{service\_name} \hfill The name of the service (up to 31 alphanumeric characters).
  \item \textit{port} \hfill The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, 22-23).
\end{itemize}

\underline{Defaults}

N/A

\underline{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

\begin{tabular}{|c|c|c|c|c|c|c|c|c|c|}
\hline
\hline
Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes \\
\hline
\end{tabular}

\underline{Usage Guidelines}

- This command is a shortcut for the \textbf{policy service protocol} command.
- Use the \textbf{no} form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The \textit{destination tcp-port} keyword may be used with this command; other keywords for the command are not allowed.)
- If the \textbf{configuration snapshot} command is entered after the \textbf{policy service} command is configured, the resulting ASCII file will include the following additional syntax for the \textbf{policy service} command:

\textbf{from \{cli | ldap | blt\}}

This syntax indicates how the service was created. The \textbf{cli} and \textbf{ldap} options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The \textbf{blt} option indicates a built-in object, this setting is not configurable.
QoS Policy Commands

policy service source tcp-port

Examples

-> policy service serv_5 source tcp-port 21-22
-> policy service serv_5 no source tcp-port

Release History

Release 7.1.1; command was introduced.

Related Commands

policy service group
Configures a policy service group, which is made up of policy services.
policy condition
Creates a policy condition.
qos apply
Applies configured QoS and policy settings to the current configuration.
show policy service
Displays information about policy services configured on the switch.

MIB Objects

alaQoSServiceTable
   alaQoSServiceName
   alaQoSServiceSource
   alaQoSServiceSourceTcpPort
   alaQoSServiceSourceTcpPortEnd
alaQoSAppliedServiceTable
   alaQoSAppliedServiceName
   alaQoSAppliedServiceSource
   alaQoSAppliedSourceTcpPort
   alaQoSAppliedSourceTcpPortEnd
**policy service destination tcp-port**

Configures a service with a destination TCP port or port range that may be used as part of a policy service group or included as part of a policy condition.

```
policy service service_name destination tcp-port port[-port]
no policy service service_name
policy service service_name no destination tcp-port
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>service_name</th>
<th>The name of the service (up to 31 alphanumeric characters).</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>The well-known port number (or port range) for the desired TCP service. For example, the port number for Telnet is 23. A port range should be separated by a hyphen (for example, 22-23).</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a service from the configuration, or to remove parameters from a particular service.

- This command is a shortcut for the `policy service protocol` command.

- A policy service may be grouped in a policy group using the `policy service group` command. A policy condition may then be associated with the service group.

- If the `configuration snapshot` command is entered after the `policy service` command is configured, the resulting ASCII file will include the following additional syntax for the `policy service` command:

```
from {cli | ldap | blt}
```

This syntax indicates how the service was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in object, this setting is not configurable.
Examples

-> policy service service4 destination tcp-port 23
-> policy service service4 no destination tcp-port

Release History

Release 7.1.1; command was introduced.

Related Commands

- **policy service group**: Configures a policy service group, which is made up of policy services.
- **policy condition**: Creates a policy condition.
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **show policy service**: Displays information about policy services configured on the switch.

MIB Objects

- **alaQoSServiceTable**
  - alaQoSServiceName
  - alaQoSServiceSource
  - alaQoSServiceDestinationTcpPort
  - alaQoSServiceDestinationTcpPortEnd
- **alaQoSAppliedServiceTable**
  - alaQoSAppliedServiceName
  - alaQoSAppliedServiceSource
  - alaQoSAppliedServiceDestinationTcpPort
  - alaQoSAppliedServiceDestinationTcpPortEnd
policy service source udp-port

Configures a service with a source UDP port or port range that may be used as part of a policy service group or included as part of a policy condition.

**policy service service_name source udp-port port[[-port]]**

**no policy service service_name**

**policy service service_name no source udp-port**

### Syntax Definitions

- **service_name**: The name of the service (up to 31 alphanumeric characters).
- **port**: The well-known port number (or port range) for the desired UDP service. Specify a port range with a hyphen (for example, 22-23).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.
- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service. Note that at least one parameter must be associated with a service.
- Ports associated with a particular service must all be of the same type. (The **destination tcp-port** keyword may be used with this command; other keywords for the command are not allowed.)
- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

  ```
  from {cli | ldap | blt}
  ```

  This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.

### Examples

```
-> policy service serv_a source udp-port 1000
```
-> no policy service serv_a source udp-port

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **policy service group**
  - Configures a policy service group, which is made up of policy services.

- **policy condition**
  - Creates a policy condition.

- **qos apply**
  - Applies configured QoS and policy settings to the current configuration.

- **show policy service**
  - Displays information about policy services configured on the switch.

**MIB Objects**

- alaQoSServiceTable
  - alaQoSServiceName
  - alaQoSServiceSource
  - alaQoSServiceSourceUdpPort
  - alaQoSServiceSourceUdpPortEnd
  - alaQoSAppliedServiceTable
    - alaQoSAppliedServiceName
    - alaQoSAppliedServiceSource
    - alaQoSAppliedSourceUdpPort
    - alaQoSAppliedSourceUdpPortEnd
**policy service destination udp-port**

Configures a service with a destination UDP port or port range that may be used as part of a policy service group or included as part of a policy condition.

```
policy service service_name destination udp-port port[-port]
no policy service service_name
policy service service_name no destination udp-port
```

### Syntax Definitions

- **service_name**: The name of the service (up to 31 alphanumeric characters).
- **port**: The well-known port number (or port range) for the desired UDP service. For example, a port number for NETBIOS is 137. A port range should be separated by a hyphen (for example, 137-138).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is a shortcut for the **policy service protocol** command.

- A policy service may be grouped in a policy group using the **policy service group** command. A policy condition may then be associated with the service group.

- Use the **no** form of the command to remove a service from the configuration, or to remove parameters from a particular service.

- If the **configuration snapshot** command is entered after the **policy service** command is configured, the resulting ASCII file will include the following additional syntax for the **policy service** command:

```
from {cli | ldap | blt}
```

This syntax indicates how the service was created. The **cli** and **ldap** options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The **blt** option indicates a built-in object, this setting is not configurable.
Examples
-> policy service service4 destination udp-port 137
-> policy service service4 no destination udp-port

Release History
Release 7.1.1; command was introduced.

Related Commands
- **policy service group**: Configures a policy service group, which is made up of policy services.
- **policy condition**: Creates a policy condition.
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **show policy service**: Displays information about policy services configured on the switch.

MIB Objects
- alaQoSServiceTable
  - alaQoSServiceName
  - alaQoSServiceSource
  - alaQoSServiceDestinationUdpPort
  - alaQoSServiceDestinationUdpPortEnd
- alaQoSAppliedServiceTable
  - alaQoSAppliedServiceName
  - alaQoSAppliedServiceSource
  - alaQoSAppliedServiceDestinationUdpPort
  - alaQoSAppliedServiceDestinationUdpPortEnd
policy condition

Creates a QoS policy condition. The condition determines what parameters the switch uses to classify incoming flows. Condition parameters may be configured when the condition is created; or parameters may be configured for an existing condition. At least one parameter must be configured for a condition.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the no form for keywords to remove a parameter from the condition.

Some condition parameters may not be supported depending on the platform you are using. Also some condition parameters may not be supported with some action parameters. See the condition/action tables in the OmniSwitch AOS Release 8 Network Configuration Guide.

```
policy condition condition_name
    [source ip ip_address [mask netmask]]
    [source ipv6 {any | ipv6_address [mask netmask]}]
    [destination ip ip_address [mask netmask]]
    [destination ipv6 {any | ipv6_address [mask netmask]}]
    [multicast ip ip_address [mask netmask]]
    [source network group network_group]
    [destination network group network_group]
    [multicast network group multicast_group]
    [source ip-port port[-port]]
    [destination ip-port port[-port]]
    [source tcp-port port[-port]]
    [destination tcp-port port[-port]]
    [source udp-port port[-port]]
    [destination udp-port port[-port]]
    [ethertype etype]
    [established]
    [tcpflags {any | all} flag [mask flag]]
    [service service]
    [service group service_group]
    [icmptype type]
    [icmpcode code]
    [ip-rotocol protocol]
    [ipv6]
    [flow-label flow_label_value]
    [tos tos_value tos_mask]
    [dscp {dscp_value[-value]} [dscp_mask]]
    [source mac mac_address [mask mac_mask]]
    [destination mac mac_address [mask mac_mask]]
    [source mac group group_name]
    [destination mac group mac_group]
    [source vlan vlan_id]
    [inner source-vlan vlan_id]
    [destination vlan vlan_id]
    [802.1p 802.1p_value]
```
[inner 802.1p 802.1p_value]  
[source port chassis/slot/port[-port2]]  
[source port group group_name]  
[destination port chassis/slot/port[-port2]]  
[destination port group group_name]  
[vrf {vrf_name | default}]  
[fragments]  
[appfp-group group_name]  
[app-mon-application-group group_name]  
[app-mon-application-name app_name]

no policy condition condition_name

## Syntax Definitions

**condition_name**

The name of the condition. Any alphanumeric string.

## Defaults

N/A

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Usage Guidelines

- A policy condition and a policy action are combined to make a policy rule. See the **policy rule** command.
- Use the **qos apply** command to activate configuration changes.
- If multiple keywords are defined for a single condition, the traffic flow must match all of the parameters in the condition before the rule is enforced.
- Use the **no** form of the command to remove a condition from a policy rule.
- At least one parameter must be associated with a condition.
- If the **configuration snapshot** command is entered after the **policy condition** command is configured, the resulting ASCII file will include the following additional syntax for the **policy condition** command:

  from {cli | ldap | blt}

This syntax indicates how the condition was created. The **cli** and **ldap** options may be changed by a
user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in condition, this option is not configurable.

**Examples**

```
-> policy condition cond4 source port 3/1/1
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `qos apply`: Applies configured QoS and policy settings to the current configuration.
- `policy action`: Configures a policy action.
- `policy rule`: Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).
- `show policy condition`: Shows information about policy conditions configured on the switch.

**MIB Objects**

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionSource`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionSource`
**policy condition source ip**

Configures a source IP address for a policy condition.

```
policy condition condition_name source ip {any | ip_address [mask netmask]}
policy condition condition_name no source ip
```

### Syntax Definitions

- `condition_name` - The name of the condition.
- `any` - Any source IPv4 address.
- `ip_address` - The source IP address of the Layer 3 flow.
- `netmask` - The mask for the source IP address.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>netmask</td>
<td>IP address class</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A source IP address and a source IP network group cannot be specified in the same condition.
- Use the `no` form of the command to remove a source IP address from a condition; however, at least one classification parameter must be associated with a condition.

### Examples

```
-> policy condition cond3 source ip 173.201.18.3
-> policy condition cond4 source ip any
```

### Release History

Release 7.1.1; command was introduced.
QoS Policy Commands

Related Commands

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy condition**
  Creates a policy condition.

- **show policy condition**
  Shows information about a particular policy condition configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionSourceIpAddr**
  - **alaQoSConditionSourceIpMask**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionSourceIpAddr**
  - **alaQoSAppliedConditionSourceIpMask**
**policy condition source ipv6**

Configures a source IPv6 address for a policy condition.

```
policy condition condition_name source ipv6 {any | ipv6_address [mask netmask]}
policy condition condition_name no source ipv6
```

### Syntax Definitions

- **condition_name**: The name of the condition.
- **any**: Any source IPv6 address.
- **ipv6_address**: A specific source IPv6 address.
- **netmask**: The mask for the source IPv6 address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove a source IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- If a mask is not specified, the IPv6 address is assumed to be a host address.
- On the OmniSwitch 6560, OmniSwitch 6570M and OmniSwitch 9900, a source IPv6 address policy condition is supported only for egress IPv6 ACLs.

### Examples

```
-> policy condition cond3 source ipv6 ::1234:531F:BCD2:F34A
-> policy condition cond4 source ipv6 any
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

**qos apply**  
Applies configured QoS and policy settings to the current configuration.

**policy condition**  
Creates a policy condition.

**show policy condition**  
Shows information about a particular policy condition configured on the switch.

MIB Objects

alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionSourceIpv6Addr
  alaQoSConditionSourceIpv6AddrStatus
  alaQoSConditionSourceIpv6Mask

alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionSourceIpv6Addr
  alaQoSAppliedConditionSourceIpv6AddrStatus
  alaQoSAppliedConditionSourceIpMask
**policy condition destination ip**

Configures a destination IP address for a policy condition.

```
policy condition condition_name destination ip ip_address [mask netmask]
policy condition condition_name no destination ip
```

**Syntax Definitions**

- `condition_name`: The name of the condition.
- `ip_address`: The source IP address of the Layer 3 flow.
- `netmask`: The mask for the source IP address.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Suitable</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a mask is not specified, the IP address is assumed to be a host address.
- A destination IP address and a destination IP network group cannot be specified in the same condition.
- Use the `no` form of the command to remove a destination IP address from a condition; however, at least one classification parameter must be associated with a condition.

**Examples**

```
-> policy condition cond4 destination ip 208.192.21.0 mask 255.255.255.0
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **policy condition**: Creates a policy condition.
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **show policy condition**: Shows information about a particular policy condition configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionDestinationIpAddr**
  - **alaQoSConditionDestinationIpMask**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionDestinationIpAddr**
  - **alaQoSAppliedConditionDestinationIpMask**
**policy condition destination ipv6**

Configures a destination IPv6 address for a policy condition.

```
policy condition condition_name destination ipv6 {any | ipv6_address [mask netmask]}
policy condition condition_name no destination ipv6
```

**Syntax Definitions**

- `condition_name` The name of the condition.
- `any` Any destination IPv6 address.
- `ipv6_address` A specific destination IPv6 address.
- `netmask` The mask for the destination IPv6 address.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a destination IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- If a mask is not specified, the IPv6 address is assumed to be a host address.
- On the OmniSwitch 6560, OmniSwitch 6570M and OmniSwitch 9900, a destination IPv6 address policy condition is supported only for *ingress* IPv6 ACLs.

**Examples**

```
-> policy condition cond3 destination ipv6 ::1234:531f:bcd2:f34a
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

qos apply  Applies configured QoS and policy settings to the current configuration.
policy condition  Creates a policy condition.
show policy condition  Shows information about a particular policy condition configured on the switch.

MIB Objects

alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionDestinationIpv6Addr
  alaQoSConditionDestinationIpv6AddrStatus
  alaQoSConditionDestinationIpv6Mask
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionDestinationIpv6Addr
  alaQoSAppliedConditionDestinationIpv6AddrStatus
  alaQoSAppliedConditionDestinationIpMask
**policy condition multicast ip**

Configures a multicast IP address for a policy condition.

```
policy condition condition_name multicast ip ip_address [mask netmask]
policy condition condition_name no multicast ip
```

### Syntax Definitions

- `condition_name` The name of the condition.
- `ip_address` The multicast IP address.
- `netmask` Optional. The mask for the multicast IP address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If a mask is not specified, the IP address is assumed to be a host address.
- A multicast IP address and a multicast network group cannot be specified in the same condition.
- Use the `no` form of the command to remove a multicast IP address from a condition; however, at least one classification parameter must be associated with a condition.

### Examples

```bash
-> policy condition cond4 multicast ip 224.1.1.1
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

**policy condition**
Creates a policy condition.

**qos apply**
Applies configured QoS and policy settings to the current configuration.

MIB Objects

alaQoSConditionTable
alaQoSConditionName
alaQoSMulticastIpAddr
alaQoSMulticastIpMask

alaQoSAppliedConditionTable
alaQoSAppliedConditionName
alaQoSAppliedMulticastIpAddr
alaQoSAppliedMulticastIpMask
**policy condition source network group**

Associates a source network group with a policy condition.

```
policy condition condition_name source network group network_group
```

```
policy condition condition_name no source network group
```

**Syntax Definitions**

- **condition_name**: The name of the condition.
- **network_group**: The name of the source network group. Network groups are configured through the `policy network group` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a source network group from a condition; however, at least one classification parameter must be associated with a condition.

- A source IP address and a source IP network group cannot be specified in the same condition.

- On the OmniSwitch 6560, OmniSwitch 6570M and OmniSwitch 9900, a source network group policy condition with an IPv6 address (includes user-configured and the built-in “Switch6” group) is supported only for egress IPv6 ACLs.

**Examples**

```
--> policy condition cond5 source network group webgroup1
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy condition**
  Creates a policy condition.

- **policy network group**
  Configures a network group name and its associated IP addresses.

- **show policy condition**
  Shows information about policy conditions configured on the switch.

- **show policy network group**
  Displays information about policy network groups.

MIB Objects

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionSourceNetworkGroup`

- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionSourceNetworkGroup`
policy condition destination network group

Associates a destination network group with a policy condition.

```
policy condition condition_name destination network group network_group
```  

```
policy condition condition_name no destination network group
```  

**Syntax Definitions**

- `condition_name`: The name of the condition.
- `network_group`: The name of the destination network group. Network groups are configured through the `policy network group` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a destination network group from a condition; however, at least one classification parameter must be associated with a condition.
- A destination IP address and a destination IP network group cannot be specified in the same condition.
- On the OmniSwitch 6560, OmniSwitch 6570M and OmniSwitch 9900, a destination network group policy condition with an IPv6 address is supported only for ingress IPv6 ACLs.

**Examples**

```
-> policy condition cond6 destination network group webgroup1
```  

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- policy condition
  Creates a policy condition.
- policy network group
  Configures a network group name and its associated IP addresses.
- qos apply
  Applies configured QoS and policy settings to the current configuration.
- show policy condition
  Shows information about policy conditions configured on the switch.
- show policy network group
  Displays information about policy network groups.

MIB Objects

alaQoSConditionTable
  - alaQoSConditionName
  - alaQoSConditionDestinationNetworkGroup
alaQoSAppliedConditionTable
  - alaQoSAppliedConditionName
  - alaQoSAppliedConditionDestinationNetworkGroup
policy condition multicast network group

Associates a multicast group with a policy condition.

policy condition condition_name multicast network group multicast_group

policy condition condition_name no multicast network group

**Syntax Definitions**

- **condition_name**: The name of the condition.
- **multicast_group**: The multicast group name. Multicast groups are configured through the `policy network group` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a multicast group from a condition; however, at least one classification parameter must be associated with a condition.

- A multicast address and a multicast network group cannot be specified in the same condition.

**Examples**

```plaintext
-> policy condition cond3 multicast group video2
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `qos apply`  Applies configured QoS and policy settings to the current configuration.
- `policy condition`  Creates a policy condition.
- `policy network group`  Configures a network group name and its associated IP addresses.
- `show policy condition`  Shows information about policy conditions configured on the switch.
- `show policy network group`  Displays information about policy network groups.

MIB Objects

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionMulticastNetworkGroup`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionMulticastNetworkGroup`
**policy condition source ip-port**

Configures a source IP port number for a policy condition.

**policy condition condition_name source ip-port \[port\]-\[port\] \**

**policy condition condition_name no source ip-port**

**Syntax Definitions**

- `condition_name`: The name of the condition.
- `port`: The TCP or UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of the command to remove a source IP port from a condition; however, at least one classification parameter must be associated with a condition.
- The protocol (TCP or UDP) must be specified in the condition, either on the same command line or in a previous command. Use the **ip-protocol** keyword. See the **policy condition ip-protocol** command.
- The same condition cannot specify a source IP port with a source TCP port, source UDP port, service, or service group.

**Examples**

```
-> policy condition cond1 ip-protocol 6 source ip-port 137
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **policy condition ip-protocol**  
  Configures an IP protocol for a policy condition.

- **show policy condition**  
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionSourceIpPort**
  - **alaQoSConditionSourceIpPortEnd**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionSourceIpPort**
  - **alaQoSAppliedConditionSourceIpPortEnd**
**policy condition destination ip-port**

Configures a destination IP port number for a policy condition.

```
policy condition condition_name destination ip-port port[-port]
policy condition condition_name no destination ip-port
```

**Syntax Definitions**

- **condition_name**: The name of the condition.
- **port**: The TCP or UDP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of the command to remove a destination IP port from a condition; however, at least one classification parameter must be associated with a condition.
- The protocol (TCP or UDP) must be specified in the same condition, either on the same command line or in a previous command. Use the **ip-protocol** keyword. See the **policy condition ip-protocol** command.
- The same condition cannot specify a destination IP port with a service or service group.

**Examples**

```
-> policy condition cond2 ip-protocol 6 destination ip-port 137-138
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.
- **policy condition ip-protocol**
  Configures an IP protocol for a policy condition.
- **show policy condition**
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionDestinationIpPort**
  - **alaQoSConditionDestinationIpPortEnd**
- **alaQoSAppliedConditionTable**
  - **alaQoSAPpliedConditionName**
  - **alaQoSAPpliedConditionDestinationIpPort**
  - **alaQoSAPpliedConditionDestinationIpPortEnd**
policy condition source tcp-port

Configures a source TCP port number for a policy condition.

```
policy condition condition_name source tcp-port port[-port]
```

```
policy condition condition_name no source tcp-port
```

**Syntax Definitions**

- `condition_name` The name of the condition.
- `port` The TCP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a source TCP port from a condition; however, at least one classification parameter must be associated with a condition.

- This command is a shortcut for the `policy condition source ip-port` command, which requires that the protocol also be specified. Rather than specifying `source ip-port` and `ip-protocol`, use `source tcp-port`.

- The same condition cannot specify a source TCP port with a service or service group.

- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.

- Use this condition in combination with the IPv6 condition (`policy condition ipv6`) to configure IPv6 policies for Layer 4 information, services, and service groups.

**Examples**

```
-> policy condition cond3 source tcp-port 137
-> policy condition cond4 ipv6 source tcp-port 21
-> policy condition cond3 no source tcp-port
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy condition ip-protocol**
  Configures an IP protocol for a policy condition.

- **show policy condition**
  Shows information about policy conditions configured on the switch.

**MIB Objects**

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aLaQoSConditionTable</td>
<td></td>
</tr>
<tr>
<td>aLaQoSConditionName</td>
<td></td>
</tr>
<tr>
<td>aLaQoSConditionSourceTcpPort</td>
<td></td>
</tr>
<tr>
<td>aLaQoSConditionSourceTcpPortEnd</td>
<td></td>
</tr>
<tr>
<td>aLaQoSAppliedConditionTable</td>
<td></td>
</tr>
<tr>
<td>aLaQoSAppliedConditionName</td>
<td></td>
</tr>
<tr>
<td>aLaQoSAppliedConditionSourceTcpPort</td>
<td></td>
</tr>
<tr>
<td>aLaQoSAppliedConditionSourceTcpPortEnd</td>
<td></td>
</tr>
</tbody>
</table>
**policy condition destination tcp-port**

Configures a destination TCP port number for a policy condition.

```
policy condition condition_name destination tcp-port port[-port]
policy condition condition_name no destination tcp-port
```

### Syntax Definitions

- **condition_name**: The name of the condition.
- **port**: The TCP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove a destination TCP port from a condition; however, at least one classification parameter must be associated with a condition.

- This command is a shortcut for the `policy condition destination ip-port` command, which requires that the protocol also be specified. Rather than specifying `destination ip-port` and `ip-protocol`, use `destination tcp-port`.

- The same condition cannot specify a destination TCP port with a service or service group.

- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.

- Use this condition in combination with the IPv6 condition (`policy condition ipv6`) to configure IPv6 policies for Layer 4 information, services, and service groups.

### Examples

```
-> policy condition cond4 destination tcp-port 137-138
-> policy condition cond5 ipv6 destination tcp-port 140
-> policy condition cond4 no destination tcp-port
```
QoS Policy Commands

Release History
Release 7.1.1; command was introduced.

Related Commands
qos apply
Applies configured QoS and policy settings to the current configuration.
policy condition ip-protocol
Configures an IP protocol for a policy condition.
show policy condition
Shows information about policy conditions configured on the switch.

MIB Objects
alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionDestinationTcpPort
  alaQoSConditionDestinationTcpPortEnd
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionDestinationTcpPort
  alaQoSAppliedConditionDestinationTcpPortEnd
**policy condition source udp-port**

Configures a source UDP port number for a policy condition.

```
policy condition condition_name source udp-port port[-port]
policy condition condition_name no source udp-port
```

### Syntax Definitions

- `condition_name`: The name of the condition.
- `port`: The UDP port number of the source address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove a source UDP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the `policy condition source ip-port` command, which requires that the protocol also be specified. Rather than specifying `source ip-port` and `ip-protocol`, use `source udp-port`.
- The same condition cannot specify a source UDP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.
- Use this condition in combination with the IPv6 condition (policy condition ipv6) to configure IPv6 policies for Layer 4 information, services, and service groups.

### Examples

- `policy condition cond5 source udp-port 1200-1400`
- `policy condition cond6 ipv6 source udp-port 1000`
- `policy condition cond5 no source udp-port`
**Release History**
Release 7.1.1; command was introduced.

**Related Commands**
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy condition ip-protocol**: Configures an IP protocol for a policy condition.
- **show policy condition**: Shows information about policy conditions configured on the switch.

**MIB Objects**
- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionSourceUdpPort**
  - **alaQoSConditionSourceUdpPortEnd**
- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionSourceUdpPort**
  - **alaQoSAppliedConditionSourceUdpPortEnd**
policy condition destination udp-port

Configures a destination UDP port number for a policy condition.

```
policy condition condition_name destination udp-port port[-port]
```

```
policy condition condition_name no destination udp-port
```

**Syntax Definitions**

- **condition_name**
  - The name of the condition.
- **port**
  - The UDP port number (or port range) of the destination address of the Layer 3 flow, in the range from 0–65535. A range of ports (separated by a hyphen) may be specified instead of a single port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a destination UDP port from a condition; however, at least one classification parameter must be associated with a condition.
- This command is a shortcut for the `policy condition destination ip-port` command, which requires that the protocol also be specified. Rather than specifying `destination ip-port` and `ip-protocol`, use `destination udp-port`.
- The same condition cannot specify a destination UDP port with a service or service group.
- IP port protocol types cannot be mixed in the same condition; ports must be either TCP or UDP.
- Use this condition in combination with the IPv6 condition (`policy condition ipv6`) to configure IPv6 policies for Layer 4 information, services, and service groups.

**Examples**

```
-> policy condition cond4 destination udp-port 137-138
-> policy condition cond5 ipv6 destination udp-port 140
-> policy condition cond4 no destination udp-port
```
Release History

Release 7.1.1; command was introduced.

Related Commands

-qos apply  Applies configured QoS and policy settings to the current configuration.
-policy condition  Creates a policy condition.
-show policy condition  Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionDestinationTcpPort
  alaQoSConditionDestinationTcpPortEnd

alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionDestinationTcpPort
  alaQoSAppliedConditionDestinationTcpPortEnd
**policy condition ethertype**

Configures an ethertype value to use for traffic classification.

```bash
policy condition condition_name ethertype etype
```

```bash
policy condition condition_name no ethertype
```

**Syntax Definitions**

- `condition_name` - The name of the condition.
- `etype` - The ethertype value, in the range 1536–65535 or 0x600–0xffff hex.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an ethertype value from a condition; however, at least one classification parameter must be associated with a condition.
- Enter a numeric or equivalent hex value for the `etype`.
- On the OmniSwitch 6465, an ethertype value is not supported in policy conditions for IPv6 packets.

**Examples**

```bash
-> policy condition cond12 ethertype 8137
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `qos apply`: Applies configured QoS and policy settings to the current configuration.
- `policy condition`: Creates a policy condition.
- `show policy condition`: Shows information about policy conditions configured on the switch.

MIB Objects

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionEthertype`
  - `alaQoSConditionEthertypeStatus`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionEthertype`
  - `alaQoSAppliedConditionEthertypeStatus`
**policy condition established**

Configures an established TCP connection as a policy condition. A connection is considered established if the **ack** or **rst** flags in the TCP header of the packet are set.

```
policy condition condition_name established
policy condition condition_name no established
```

**Syntax Definitions**

| condition_name         | The name of the condition. |

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove **established** from a condition; however, at least one classification parameter must be associated with a condition.
- When an initial TCP connection packet is received only the **syn** flag is set. As a result, TCP packets are only examined if they are not the starting packet.
- Typically this condition is used in combination with **source ip**,** destination ip**,** source port**,** destination port**,** source tcp-port**,** destination tcp-port** conditions.
- Note that even though **established** can be used with most action parameters, it is mainly intended for ACL use.

**Examples**

```
-> policy condition cond2 source ip 192.168.5.10 established
-> policy condition cond3 destination ip 10.255.11.40
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **policy condition**  
  Creates a policy condition.

- **show policy condition**  
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionTcpEstablished**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionTcpEstablished**
**policy condition tcpflags**

Configures a specific TCP flag value or combination of flag values as a policy condition.

```
policy condition condition_name tcpflags [any | all] \{f | s | r | p | a | u | e | w\} mask \{f | s | r | p | a | u | e | w\}
policy condition condition_name no tcpflags
```

**Syntax Definitions**

- `condition_name`: The name of the condition.
- `any`: Match on any of the specified TCP flags.
- `all`: Match all specified TCP flags.
- `f | s | r | p | a | u | e | w`: TCP flag value to match (f=fin, s=syn, r=rst, p=psh, a=ack, u=urg, e=ecn, and w=cwr). *The e and w flags are currently not supported.*

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>all</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of the command to remove **tcpflags** from a condition; however, at least one classification parameter must be associated with a condition.

- Use the **any** option to indicate that a match on any one of the specified TCP flags qualifies as a match for the condition. Use the **all** option to indicate that a match on all specified TCP flags is required to qualify as a match for the condition.

- Enter one or more TCP flags after the **any** or **all** keyword to indicate that the value of the flag bit must be set to one to qualify as a match.

- Enter one or more TCP flags after the **mask** keyword to indicate which TCP flags to match.

- If a TCP flag is specified as part of the **mask** but does not have a corresponding match value specified with the **any** or **all** options, then zero is assumed as the match value. For example, **tcpflags all f s mask f s a** looks for the following bit values to determine a match: f=1, s=1, a=0.
• Typically this condition is used in combination with source ip, destination ip, source port, destination port, source tcp-port, or destination tcp-port conditions.

• Note that even though tcpflags can be used with most action parameters, it is mainly intended for ACL use.

• Use tcpflags in combination with the IPv6 condition to configure an IPv6 TCP flag policy (for example, policy condition ipv6 tcpflags). Note that IPv6 TCP flag conditions are not supported on the OmniSwitch 6560 and OmniSwitch 6570M.

Examples

-> policy condition tcp-flag tcpflags all f s mask f s a
-> policy condition tcp-flag-ar tcpflags any a r mask a r
-> policy condition tcp-flag-f destination network group Allowed_Resources source tcp-port 1982 tcpflags any f mask f ipv6

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply | Applies configured QoS and policy settings to the current configuration.
policy condition | Creates a policy condition.
show policy condition | Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable

alaQoSConditionTable
alaQoSConditionTcpFlags,
alaQoSConditionTcpFlagsStatus,
alaQoSConditionTcpFlagsVal,
alaQoSConditionTcpFlagsValStatus,
alaQoSConditionTcpFlagsMask,
alaQoSConditionTcpFlagsMaskStatus,
alaQoSAppliedConditionTable
alaQoSAppliedConditionTcpFlags,
alaQoSAppliedConditionTcpFlagsStatus,
alaQoSAppliedConditionTcpFlagsVal,
alaQoSAppliedConditionTcpFlagsValStatus,
alaQoSAppliedConditionTcpFlagsMask,
alaQoSAppliedConditionTcpFlagsMaskStatus,
**policy condition service**

Configures a service for a policy condition.

```
policy condition condition_name service service_name
policy condition condition_name no service
```

**Syntax Definitions**

- `condition_name` The name of the condition.
- `service_name` The service name, configured through the `policy service` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a service group from a condition; however, at least one classification parameter must be associated with a condition.

- A policy condition that specifies a service cannot also specify a service group, IP protocol, source IP port, or destination IP port.

**Examples**

```
-> policy condition cond12 service serv2
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **policy service**: Configures a service that may be used as part of a policy service group.
- **qos apply**: Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
- **show policy service**: Displays information about all particular policy services or a particular policy service configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionService**
- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionService**
**policy condition service group**

Associates a policy service group with a policy condition.

```plaintext
policy condition condition_name service group service_group

policy condition condition_name no service group
```

**Syntax Definitions**

- `condition_name`:
  The name of the condition.

- `service_group`:
  The service group name. Service groups are configured through the `policy service group` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900/V72/C32</th>
<th>6900/X48C6/T48C6/</th>
<th>6900/X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a service group from a condition; however, at least one classification parameter must be associated with a condition.

- A policy condition that specifies a service group cannot also specify a service, IP protocol, source IP port, or destination IP port.

**Examples**

```plaintext
-> policy condition cond12 service group servgroup2
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **policy service group**: Configures a service group and its associated services.
- **policy condition**: Creates a policy condition.
- **qos apply**: Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
- **show policy condition**: Shows information about policy conditions configured on the switch.

MIB Objects

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionServiceGroup`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionServiceGroup`
**policy condition icmptype**

Configures an ICMP type value to use for traffic classification.

```
policy condition condition_name icmptype type
policy condition condition_name no icmptype
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>condition_name</th>
<th>The name of the condition.</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>The ICMP type value, in the range 0–255.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of the command to remove an ICMP type value from a condition; however, at least one classification parameter must be associated with a condition.

**Examples**

```
-> policy condition cond12 icmptype 100
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `policy condition icmpcode` Configures an ICMP code value for traffic classification.
- `policy condition` Creates a policy condition.
- `qos apply` Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
- `show policy condition` Shows information about policy conditions configured on the switch.

MIB Objects

- `alaQoSConditionTable` 
  - `alaQoSConditionName`
  - `alaQoSConditionIcmpType`
  - `alaQoSConditionIcmpTypeStatus`
- `alaQoSAppliedConditionTable` 
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionIcmpType`
  - `alaQoSAppliedConditionIcmpTypeStatus`
**policy condition icmpcode**

Configures an ICMP code value to use for traffic classification.

```
policy condition condition_name icmpcode code
```

```
policy condition condition_name no icmpcode
```

### Syntax Definitions

- **condition_name**: The name of the condition.
- **code**: The ICMP code value, in the range 0–255.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **no** form of the command to remove an ICMP code value from a condition; however, at least one classification parameter must be associated with a condition.

### Examples

```
-> policy condition cond12 icmpcode 150
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **policy condition icmptype** Configures an ICMP type value for traffic classification.
- **policy condition** Creates a policy condition.
- **qos apply** Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
- **show policy condition** Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionIcmpCode**
  - **alaQoSConditionIcmpCodeStatus**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionIcmpCode**
  - **alaQoSAppliedConditionIcmpCodeStatus**
**policy condition ip-protocol**

Configures an IP protocol for a policy condition.

`policy condition condition_name ip-protocol protocol`

`policy condition condition_name no ip-protocol`

---

**Syntax Definitions**

- `condition_name`: The name of the condition.
- `protocol`: The protocol associated with the flow. The range is 0–255.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>6</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of the command to remove a protocol from a condition; however, at least one classification parameter must be associated with a condition.

- If a source or destination port is specified (through the `policy condition source ip-port` or `policy condition destination ip-port` commands), the protocol must be specified.

- The same condition cannot specify an IP protocol with a service or service group.

---

**Examples**

`-> policy condition cond4 ip-protocol 6`

---

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **policy condition source ip-port**  Configures a source IP port number for a policy condition.
- **policy condition destination ip-port**  Configures a destination IP port number for a policy condition.
- **qos apply**  Applies configured global QoS and policy settings to the current configuration (changes will be active and stored in flash).
- **show policy condition**  Shows information about policy conditions configured on the switch.

**MIB Objects**

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionIpProtocol**
- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionIpProtocol**
policy condition ipv6

Configures a policy condition to classify IPv6 traffic.

```
policy condition condition_name ipv6
```

```
policy condition condition_name no ipv6
```

### Syntax Definitions

*condition_name*  
The name of the condition.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the *no* form of the command to remove IPv6 traffic as a condition; however, at least one classification parameter must be associated with a condition.

- When the *ipv6* keyword is used in a condition, a policy that uses the condition is considered an IPv6 policy. IPv6 policies are effected only on IPv6 traffic. All other IP policies are considered IPv4 policies and are effected only on IPv4 traffic.

- IPv6 Layer 4 policies are supported and are configured using the *ipv6* keyword in a condition that specifies Layer 4 information, services, or service groups. Note that IPv6 Layer 4 policies only work with packets that contain a single header.

- The *icmptype* and *icmpcode* keywords in an IPv6 policy imply the ICMPv6 protocol, not the ICMPv4 protocol.

### Examples

```
-> policy condition cond4 ipv6
-> policy condition cond5 ipv6 tos 7
-> policy condition cond6 ipv6 source port 1/1/1
-> policy condition cond7 ipv6 source tcp-port 21
-> policy condition cond8 ipv6 source tcp-port 0-1024
-> policy condition cond6 no ipv6
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `qos apply`  
  Applies configured QoS and policy settings to the current configuration.
- `show policy condition`  
  Shows information about policy conditions configured on the switch.

**MIB Objects**

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionIpv6Traffic`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionIpv6Traffic`
policy condition flow-label

Configures an IPv6 flow label value as a policy condition. This value is compared to the flow label value in the IPv6 header.

```
policy condition condition_name flow-label flow_label_value
policy condition condition_name no flow-label
```

### Syntax Definitions

- **condition_name**
  - The name of the condition.

- **flow_label_value**
  - The flow-label value (0–1048575).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **no** form of the command to remove the flow label value as a condition; however, at least one classification parameter must be associated with a condition.

### Examples

```
-> policy condition cond4 flow-label 1500
-> policy condition cond4 no flow-label
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

qos apply  
Applies configured QoS and policy settings to the current configuration.

show policy condition  
Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
   alaQoSConditionName
   alaQoSConditionIpv6FlowLabel
   alaQoSConditionIpv6FlowLabelStatus

alaQoSAppliedConditionTable
   alaQoSAppliedConditionName
   alaQoSAppliedConditionIpv6FlowLabel
   alaQoSAppliedConditionIpv6FlowLabelStatus
**policy condition tos**

Configures the precedence bits in the Type of Service (ToS) byte value for a policy condition.

```
policy condition condition_name tos tos_value [mask tos_mask]
policy condition condition_name no tos
```

### Syntax Definitions

- `condition_name` - The name of the condition. May be an existing condition name or a new condition.
- `tos_value` - The Type of Service bits value included in the IP header. The three most significant bits of the byte determine the precedence (i.e., priority) of the frame (0 is the lowest, 7 is the highest).
- `tos_mask` - The mask for the ToS bits, in the range 0–7.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove a ToS value from a condition; however, at least one classification parameter must be associated with a condition.
- If a ToS value is specified, a DSCP value may not be specified.

### Examples

```
-> policy condition cond2 tos 7
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **policy condition**: Creates a policy condition.
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **show policy condition**: Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionTos**
- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionTos**
**policy condition dscp**

Configures the Differentiated Services Code Point (DSCP) for a policy condition. The DSCP value defines the six most significant bits of the DS byte in the IP header.

```
policy condition condition_name dscp {dscp_value[-value]} [mask dscp_mask]
policy condition condition_name no dscp
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th><code>condition_name</code></th>
<th>The name of the condition. May be an existing condition name or a new condition.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dscp_value[-value]</code></td>
<td>The DiffServ Code Point value, in the range 0–63. Use a hyphen to specify a range of DSCP values for the condition (for example, 10-20).</td>
</tr>
<tr>
<td><code>dscp_mask</code></td>
<td>The mask for the DiffServ Code Point, in the range 0–63. Specifying a DSCP mask for a policy condition is not supported on an OmniSwitch 6360 or OmniSwitch 6465.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a DSCP value from a condition; however, at least one classification parameter must be associated with a condition.
- If a DSCP value is specified, a ToS value may not be specified.
- When a DSCP policy condition is configured on one of these switches, QoS automatically calculates the appropriate mask value.

**Examples**

```
-> policy condition cond4 dscp 10
-> policy condition cond5 dscp 20-30
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **policy condition**  
  Creates a policy condition.

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **show policy condition**  
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionDscp**
  - **alaQoSConditionDscpMask**
  - **alaQoSConditionDscpEnd**
  - **alaQoSConditionDscpStatus**

- **alaQosAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionDscp**
  - **alaQoSAppliedConditionDscpMask**
  - **alaQoSAppliedConditionDscpEnd**
  - **alaQoSAppliedConditionDscpStatus**
**policy condition source mac**

Configures a source MAC address for a policy condition.

```
policy condition condition_name source mac mac_address [mask mac_mask]
policy condition condition_name no source mac
```

**Syntax Definitions**

- **condition_name**: The name of the condition. May be an existing condition name or a new condition.
- **mac_address**: The source MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23)
- **mac_mask**: Optional. The mask for the source MAC address (for example, ff:ff:ff:ff:ff:ff).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a source MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- A source MAC address and a source MAC group cannot be specified in the same condition.
- On the OmniSwitch 6465, a source MAC address is not supported in policy conditions for IPv6 packets.

**Examples**

```
-> policy condition cond2 source mac 00:20:da:05:f6:23
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

qos apply           Applies configured QoS and policy settings to the current configuration.
policy condition   Creates a policy condition.
show policy condition Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionSourceMacAddr
  alaQoSConditionSourceMacMask
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionSourceMacAddr
  alaQoSAppliedConditionSourceMacMask
**policy condition destination mac**

Configures a destination MAC address for a policy condition.

Specifying a destination MAC address and mask of all zeros (00:00:00:00:00:00) as a policy condition can result in the switch dropping all traffic. Only use this type of condition in combination with other policies that will allow desired traffic and/or if a source or destination slot/port is also part of the destination MAC condition.

```
policy condition condition_name destination mac [mask mac_mask]
policy condition condition_name no destination mac
```

**Syntax Definitions**

- `condition_name` The name of the condition. May be an existing condition name or a new condition.
- `mac_address` The destination MAC address in the Layer 2 header of the frame (for example, 00:20:da:05:f6:23).
- `mac_mask` Optional. The mask for the destination MAC address (for example, ff:ff:ff:ff:ff:ff).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a destination MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- A destination MAC address and a destination MAC group cannot be specified in the same condition.
- On the OmniSwitch 6465, a destination MAC address is not supported in policy conditions for IPv6 packets.

**Examples**

```
-> policy condition cond3 destination mac 00:20:da:05:f6:23
```
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.
- **policy condition**  
  Creates a policy condition.
- **show policy condition**  
  Shows information about policy conditions configured on the switch.

**MIB Objects**

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionSource`
  - `alaQoSConditionDestinationMacAddr`
  - `alaQoSConditionDestinationMacMask`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionSource`
  - `alaQoSAppliedConditionDestinationMacAddr`
  - `alaQoSAppliedConditionDestinationMacMask`
**policy condition source mac group**

Associates a source MAC group with a policy condition.

```
policy condition condition_name source mac group group_name
policy condition condition_name no source mac group
```

### Syntax Definitions

- **condition_name**
  - The name of the condition. May be an existing condition name or a new condition.

- **group_name**
  - The name of the source MAC group, configured through the `policy mac group` command.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove a source MAC group from a condition; however, at least one classification parameter must be associated with a condition.

- A source MAC address and a source MAC group cannot be specified in the same condition.

- On the OmniSwitch 6465, a source MAC group is not supported in policy conditions for IPv6 packets.

### Examples

```
-> policy condition cond4 source mac group mac_group1
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **qos apply** Applies configured QoS and policy settings to the current configuration.
- **policy mac group** Configures a MAC group and its associated MAC addresses.
- **policy condition** Creates a policy condition.
- **show policy condition** Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionSourceMacGroup**
- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionSourceMacGroup**
**policy condition destination mac group**

Associates a destination MAC group with a policy condition.

```
policy condition condition_name destination mac group mac_group
```

```
policy condition condition_name no destination
```

---

**Syntax Definitions**

- `condition_name`: The name of the condition. May be an existing condition name or a new condition.
- `mac_group`: The name of the destination MAC group, configured through the `policy mac group` command.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of the command to remove a destination MAC group from a policy condition; however, at least one classification parameter must be associated with a condition.
- A destination MAC address and a destination MAC group cannot be specified in the same condition.
- On the OmniSwitch 6465, a source MAC group is not supported in policy conditions for IPv6 packets.

---

**Examples**

```
-> policy condition cond5 destination mac group mac_group1
```

---

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy mac group**: Configures a MAC group and its associated MAC addresses.
- **policy condition**: Creates a policy condition.
- **show policy condition**: Shows information about policy conditions configured on the switch.

**MIB Objects**

alaQoSConditionTable
- alaQoSConditionName
- alaQoSConditionDestinationMacGroup

alaQoSAppliedConditionTable
- alaQoSAppliedConditionName
- alaQoSAppliedConditionDestinationMacGroup
**policy condition source vlan**

Configures a source VLAN for a policy condition.

```
policy condition condition_name source vlan vlan_id
```

```
policy condition condition_name no source vlan
```

### Syntax Definitions

- **condition_name**: The name of the condition. May be an existing condition name or a new condition.
- **vlan_id**: The source VLAN ID for the flow.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **no** form of the command to remove a source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.

### Examples

```
-> policy condition cond5 source vlan 3
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

- `qos apply`  Applies configured QoS and policy settings to the current configuration.
- `policy condition`  Creates a policy condition.
- `show policy condition`  Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  - `alaQoSConditionName`
  - `alaQoSConditionSourceVlan`
alaQoSAppliedConditionTable
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionSourceVlan`
**policy condition inner source-vlan**

Configures an inner source VLAN ID as a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner VLAN ID tag, also known as the customer VLAN ID.

**Syntax**

```
policy condition condition_name inner source-vlan vlan_id
policy condition condition_name no inner source-vlan
```

**Syntax Definitions**

- `condition_name` The name of the condition. May be an existing condition name or a new condition.
- `vlan_id` The inner source VLAN ID (customer VLAN ID) to match on double-tagged packets.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove an inner source VLAN from a policy condition; however, at least one classification parameter must be associated with a condition.

- Policies that use the inner source VLAN condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.

**Examples**

```
-> policy condition cond5 inner source-vlan 3
-> policy condition cond5 no inner source-vlan
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- `qos apply`  Applies configured QoS and policy settings to the current configuration.
- `policy condition`  Creates a policy condition.
- `show policy condition`  Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionInnerSourceVlan
  alaQoSConditionInnerSourceVlanStatus
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionInnerSourceVlan
  alaQoSAppliedConditionInnerSourceVlanStatus
**policy condition destination vlan**

Configures a destination VLAN (multicast only) for a policy condition.

```plaintext
policy condition condition_name destination vlan vlan_id
policy condition condition_name no destination vlan
```

**Syntax Definitions**

- `condition_name`  The name of the condition. May be an existing condition name or a new condition.
- `vlan_id`  The destination VLAN ID for the flow.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900v72/c32</th>
<th>6900v82/c32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a destination VLAN from a condition; however, at least one classification parameter must be associated with a condition.
- Note that this condition is supported for multicast only policies.

**Examples**

```plaintext
-> policy condition cond4 destination vlan 3 multicast ip any
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**
  - Applies configured QoS and policy settings to the current configuration.

- **policy condition**
  - Creates a policy condition.

- **show policy condition**
  - Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionDestinationVlan**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionDestinationVlan**
**policy condition 802.1p**

Configures the 802.1p value for a policy condition.

```
policy condition condition_name 802.1p 802.1p_value
policy condition condition_name no 802.1p
```

---

**Syntax Definitions**

- **condition_name**
  - The name of the condition. May be an existing condition name or a new condition.

- **802.1p_value**
  - The 802.1p value in the 802.1Q VLAN tag for the flow. Values range from 0 (lowest priority) to 7 (highest priority).

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the **no** form of the command to remove an 802.1p value for a condition; however, at least one classification parameter must be associated with a condition.

---

**Examples**

```
-> policy condition cond3 802.1p 7
```

---

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy condition**: Creates a policy condition.
- **show policy condition**: Shows information about policy conditions configured on the switch.

**MIB Objects**

- `alaQoSCConditionTable`
  - `alaQoSCConditionName`
  - `alaQoSCCondition8021p`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedCondition8021p`
policy condition inner 802.1p

Configures an inner (customer) source 802.1p value for a policy condition. This condition applies to double-tagged VLAN Stacking traffic and is used to classify such traffic based on the inner 802.1p bit value.

`policy condition condition_name inner 802.1p 802.1p_value`

`policy condition condition_name no inner 802.1p`

**Syntax Definitions**

- `condition_name`: The name of the condition. May be an existing condition name or a new condition.
- `802.1p_value`: The inner 802.1p value of the inner 802.1Q VLAN tag (customer VLAN) to match on double-tagged packets. Values range from 0 (lowest priority) to 7 (highest priority).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove an 802.1p value for a condition; however, at least one classification parameter must be associated with a condition.

- Policies that use the inner 802.1p condition are referred to as QoS VLAN Stacking policies. These are separate policies from those configured through the VLAN Stacking Service application.

**Examples**

- `-> policy condition cond3 inner 802.1p 7`
- `-> policy condition cond3 no inner 802.1p`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy condition**
  Creates a policy condition.

- **show policy condition**
  Shows information about policy conditions configured on the switch.

**MIB Objects**

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionInner8021p`
  - `alaQoSConditionInner8021pStatus`

- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionInner8021p`
  - `alaQoSAppliedConditionInner8021pStatus`
**policy condition source port**

Configures a source port number for a policy condition. Use the **no** form of the command to remove a source port number from a condition.

```
policy condition condition_name source {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
policy condition condition_name no source {port | linkagg}
```

**Syntax Definitions**

- **condition_name**: The name of the condition. May be an existing condition name or a new condition.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number on which the frame is received. Use a hyphen to specify a range of ports (1/5-10). **Specifying a range of ports for a policy condition is not supported on an OmniSwitch 6360 or OmniSwitch 6465.**
- **agg_id[-agg_id2]**: The link aggregate ID on which the frame is received. Use a hyphen to specify a range of IDs (10-15). **A link aggregate policy condition is not supported on the OmniSwitch 6560, OmniSwitch 6570M, OmniSwitch 6900-V72/C32, and OmniSwitch 9900.**

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **no** form of the command to remove a source port from a condition; however, at least one classification parameter must be associated with a condition.

**Examples**

- `policy condition cond2 source port 3/1/1`
- `policy condition cond3 source port 3/2/1-4`
- `policy condition cond3 no source port`
- `policy condition cond3 source linkagg 10`
- `policy condition cond3 source linkagg 15-20`
- `policy condition cond3 no source linkagg`
Release History

Release 7.1.1; command was introduced.
Release 8.3.1; linkagg parameter added.

Related Commands

- qos apply: Applies configured QoS and policy settings to the current configuration.
- policy condition: Creates a policy condition.
- show policy condition: Shows information about policy conditions configured on the switch.

MIB Objects

- alaQoSConditionTable
  - alaQoSConditionName
  - alaQoSConditionSourceSlot
  - alaQoSConditionSourcePort
  - alaQoSConditionSourcePortEnd
  - alaQoSConditionSourceChassis

- alaQoSAppliedConditionTable
  - alaQoSAppliedConditionName
  - alaQoSAppliedConditionSourceSlot
  - alaQoSAppliedConditionSourcePort
  - alaQoSAppliedConditionSourcePortEnd
  - alaQoSAppliedConditionSourceChassis
policy condition destination port

Configures a destination port number for a policy condition.

policy condition condition_name destination {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}

policy condition condition_name no destination {port | linkagg}

Syntax Definitions

| condition_name | The name of the condition. May be an existing condition name or a new condition.
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port[-port2]</td>
<td>The slot and port number for which the frame is destined. Use a hyphen to specify a range of ports (1/5-10).</td>
</tr>
<tr>
<td>agg_id[-agg_id2]</td>
<td>The link aggregate ID for which the frame is destined. Use a hyphen to specify a range of IDs (10-15). A link aggregate policy condition is not supported on the OmniSwitch 6900-V72/C32 and OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of the command to remove a destination port from a condition; however, at least one classification parameter must be associated with a condition.
- The destination port condition does not apply to routed traffic. Only bridged unicast traffic is supported (bridged multicast and broadcast traffic is not supported).
- On an OmniSwitch 9900, a destination port condition is supported only when the condition is part of a policy rule that was configured using the no default-list option (for example, policy rule r1 condition c1 action a1 no default-list) and the rule is assigned to an egress policy list.

Examples

-> policy condition cond3 destination port 4/2/1
-> policy condition cond4 destination port 4/3/1-4
-> policy condition cond4 no destination port
QoS Policy Commands

-> policy condition cond4 destination linkagg 10
-> policy condition cond4 destination linkagg 15-20
-> policy condition cond4 no destination linkagg

On the OmniSwitch 9900, a destination port condition is supported only with the following configuration of the policy rule:

-> policy condition cond5 destination port 1/3/1
-> policy action a1
-> policy rule r1 condition cond5 action a1 no default-list
-> policy list list1 type egress
-> policy list list1 rules r1
-> qos apply

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; linkagg parameter added.

Related Commands

qos apply       Applies configured QoS and policy settings to the current configuration.
policy condition Creates a policy condition.
show policy condition Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  alaQoSConditionName
  alaQoSConditionDestinationSlot
  alaQoSConditionDestinationPort
  alaQoSConditionDestinationPortEnd
  alaQoSConditionDestinationChassis
alaQoSAppliedConditionTable
  alaQoSAppliedConditionName
  alaQoSAppliedConditionDestinationSlot
  alaQoSAppliedConditionDestinationPort
  alaQoSAppliedConditionDestinationPortEnd
  alaQoSAppliedConditionDestinationChassis
**policy condition source port group**

Associates a source port group with a policy condition. Use the no form of the command to remove a source port group from a condition.

```
policy condition condition_name source port group group_name
```

```
policy condition condition_name no source port group
```

**Syntax Definitions**

- **condition_name**: The name of the condition. May be an existing condition name or a new condition.
- **group_name**: The name of the source port group. Port groups are configured through the `policy port group` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the no form of the command to remove a source port group from a condition; however, at least one classification parameter must be associated with a condition.

**Examples**

```
-> policy condition cond6 source port group portgr4
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **policy port group**: Configures a port group and its associated slot and port numbers.
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy condition**: Creates a policy condition.
- **show policy condition**: Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionSourcePortGroup**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionSourcePortGroup**
**policy condition destination port group**

Associates a destination port group with a policy condition. Use the `no` form of the command to remove a destination port group from a condition.

```
policy condition condition_name destination port group group_name
policy condition condition_name no destination port
```

**Syntax Definitions**

- `condition_name`: The name of the condition. May be an existing condition name or a new condition.
- `group_name`: The name of the destination port group. Port groups are configured through the `policy port group` command.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of the command to remove a destination port group from a condition; however, at least one classification parameter must be associated with a condition.

**Examples**

```
-> policy condition cond6 destination port group portgr4
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **policy port group**: Configures a port group and its associated slot and port numbers.
- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy condition**: Creates a policy condition.
- **show policy condition**: Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionDestinationPortGroup**
- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionDestinationPortGroup**
policy condition vrf

Associates a Virtual Routing and Forwarding (VRF) instance with a policy condition.

```
policy condition condition_name vrf {vrf_name | default}
policy condition condition_name no vrf
```

Syntax Definitions

- **condition_name**: The name of the condition. May be an existing condition name or a new condition.
- **vrf_name**: The name of the VRF instance to which the QoS policy condition applies.
- **default**: Specifies the default VRF instance.

Defaults

By default, QoS policy conditions are not associated with any VRF instance. The policy applies across all instances.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of the command to remove a VRF instance from a condition; however, at least one classification parameter must be associated with a condition.
- VRF policies are configured in the default VRF, similar to how all other QoS policies are configured. If the VRF name specified does not exist, the policy is not allocated any system resources.
- Policies that do not specify a VRF name are considered global policies and are applied across all VRF instances and VLANs.
- Policies that specify the default VRF apply only to traffic in the default VRF instance.
- Policies that specify a VRF name apply only to traffic in the VRF instance associated with that name.
- The switch network group is supported only in VRF policies that specify the default VRF instance. If this group is specified in a global policy (no VRF specified) then the policy is applied across all VRF instances.
**Examples**

- `policy condition cond6 vrf engr-vrf`
- `policy condition cond7 vrf default`
- `policy condition cond6 no vrf`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `qos apply` Applies configured QoS and policy settings to the current configuration.
- `policy condition` Creates a policy condition.
- `show policy condition` Shows information about policy conditions configured on the switch.

**MIB Objects**

- `alaQoSConditionTable`
  - `alaQoSConditionName`
  - `alaQoSConditionVrfName`
  - `alaQoSConditionVrfNameStatus`
- `alaQoSAppliedConditionTable`
  - `alaQoSAppliedConditionName`
  - `alaQoSAppliedConditionVrfName`
  - `alaQoSAppliedConditionVrfNameStatus`
policy condition fragments

Associates TCP packet fragments with a policy condition.

policy condition condition_name fragments

policy condition condition_name no fragments

**Syntax Definitions**

*condition_name*  
The name of the condition. May be an existing condition name or a new condition.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of the command to remove TCP packet fragments from a condition; however, at least one classification parameter must be associated with a condition.

**Examples**

- `-> policy condition cond6 fragments`
- `-> policy condition cond7 no fragments`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **policy condition**  
  Creates a policy condition.

- **show policy condition**  
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionName**
  - **alaQoSConditionFragments**

- **alaQoSAppliedConditionTable**
  - **alaQoSAppliedConditionName**
  - **alaQoSAppliedConditionFragments**
policy condition app-mon-application-group

Associates an Application Monitoring and Enforcement (AppMon) application group with a policy condition.

policy condition condition_name app-mon-application-group group_name

policy condition condition_name no app-mon-application-group

Syntax Definitions

condition_name
The name of the condition. May be an existing condition name or a new condition.

group_name
The name of the AppMon application group to which the QoS policy condition applies.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of the command to remove an AppMon group name from a condition; however, at least one classification parameter must be associated with a condition.

- The app-mon-application-group policy condition is used in the rules associated with QoS default policy lists or UNP policy lists.

- Policy condition command will not support any other native QoS policy condition keywords along with AppMon application group or name keyword.

- For more information about AppMon, see the “Configuring Application Monitoring and Enforcement” chapter in the OmniSwitch AOS Release 8 Network Configuration Guide.

Examples

-> policy condition cond6 app-mon-application-group web
-> policy condition cond6 no app-mon-application-group

Release History

Release 8.2.1; command was introduced.
Related Commands

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy condition**
  Creates a policy condition.

- **show policy condition**
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionDpiAppGroup**
  - **alaQoSConditionDPIAppGroupStatus**
policy condition app-mon-application-name

Associates an Application Monitoring and Enforcement (AppMon) application name with a policy condition.

```
policy condition condition_name app-mon-application-name app_name
policy condition condition_name no app-mon-application-name
```

**Syntax Definitions**

- **condition_name**
  - The name of the condition. May be an existing condition name or a new condition.

- **app_name**
  - The name of the AppMon application to which the QoS policy condition applies.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove an AppMon application name from a condition; however, at least one classification parameter must be associated with a condition.

- The `app-mon-application-group` policy condition is used in the rules associated with QoS default policy lists or UNP policy lists.

- Policy condition command will not support any other native QoS policy condition keywords along with AppMon application group or name keyword.

- For more information about AppMon, see the “Configuring Application Monitoring and Enforcement” chapter in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

**Examples**

```
-> policy condition cond6 app-mon-application-name whatsapp
-> policy condition cond6 no app-mon-application-name
```

**Release History**

Release 8.2.1; command was introduced.
Related Commands

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **policy condition**  
  Creates a policy condition.

- **show policy condition**  
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**  
  - **alaQoSConditionDPIAppName**  
  - **alaQoSConditionDPIAppNameStatus**
**policy condition appfp-group**

Associates an Application Fingerprinting (AFP) application signature group with a policy condition.

```
policy condition condition_name appfp-group group_name
```

```
policy condition condition_name no appfp-group
```

### Syntax Definitions

- **condition_name**: The name of the condition. May be an existing condition name or a new condition.
- **group_name**: The name of the AFP application group to which the QoS policy condition applies.

### Defaults

N/A.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove an AFP group name from a condition; however, at least one classification parameter must be associated with a condition.
- The `appfp-group` policy condition is used in rules associated with QoS policy lists that are applied to AFP ports running in either the QoS or UNP mode.

### Examples

```
-> policy condition cond6 appfp-group my-p2p
```

```
-> policy condition cond6 no appfp-group
```

### Release History

Release 7.3.2; command was introduced.
Related Commands

- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy condition**: Creates a policy condition.
- **show policy condition**: Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  - alaQoSConditionAppFpGroup
  - alaQoSConditionAppFpGroupStatus
**policy condition vxlan**

Creates a VXLAN Snooping policy condition to determine the parameters the switch uses to classify incoming encapsulated Virtual eXtensible Local Area Network (VXLAN) packets. Condition parameters may be configured when the condition is created; or parameters may be configured for an existing condition. At least one parameter must be configured for a condition.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the `no` form for keywords to remove a parameter from the condition.

```plaintext
policy condition condition_name vxlan vni vxlan_id
    [inner source mac mac_address [mask mac_mask]]
    [inner source mac-group mac_group]
    [inner source ip ip_address [mask netmask]]
    [inner source ipv6 ip6_address [mask netmask]]
    [inner ip-protocol protocol]
    [inner l4-port {src src_port | dest dest_port}]
    [vxlan-port udp_port]
```

**Syntax Definitions**

- **condition_name**
  - The name of the VXLAN condition. Any alphanumeric string.

- **vxlan_id**
  - A 24-bit numerical value that identifies traffic for a VXLAN segment. The valid range is 1–2147483647.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A policy condition and a policy action are combined to make a policy rule. See the `policy rule` command.
- Use the `qos apply` command to activate configuration changes.
- If multiple keywords are defined for a single condition, the traffic flow must match all of the parameters in the condition before the rule is enforced.
Use the **no** form of the command to remove a condition from the switch configuration.

The **vni** (VXLAN Network Identifier) parameter is required to configure a VM Snooping policy condition. The VXLAN header contains the VNI that is associated with the source MAC address of the Ethernet frame that is encapsulated in a VXLAN packet. The VNI represents the VXLAN segment ID to which the packet belongs.

The **vxlan-port** condition parameter applies only to the outer header of an encapsulated VXLAN packet. All other **inner** condition parameters apply only to the inner header of the Ethernet frame that was encapsulated in a VXLAN packet.

When a VXLAN Snooping policy condition is used in a policy rule, the rule is then applied only to traffic on ports that have the VM Snooping feature enabled.

All existing policy actions are supported in combination with VXLAN Snooping policy conditions; there are no specific policy actions required for policy rules containing VXLAN Snooping policy conditions. Policy actions are applied to the outer header of an encapsulated VXLAN packet.

See the “Configuring VXLAN Snooping” chapter in the *OmniSwitch AOS Release 8 Data Center Switching Guide* for more information about using VXLAN Snooping policy rules.

**Examples**

```
-> policy condition cond4 vxlan vni 23000
```

The following is an example of using VM Snooping policy conditions in a policy rule that is added to a UNP policy list:

```
-> policy condition c1 vxlan vni 1234 udp-port 4789
-> policy condition c1 vxlan inner source mac 00:11:22:33:44:00
-> policy condition c1 vxlan inner source ip 10.10.10.10
-> policy action a1 disposition dscp 45
-> policy rule r1 condition c1 action a1 no default-list
-> policy list list1 type UNP
-> policy list list1 rule r1
-> qos apply
```

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy action**
  Configures a policy action.

- **policy rule**
  Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

- **show policy condition**
  Shows information about policy conditions configured on the switch.
MIB Objects

alaQoSConditionTable
  alaQoSConditionVxlanVni
  alaQoSConditionVxlanVniStatus
  alaQoSConditionVxlanPort
  alaQoSConditionVmSourceMacAddr
  alaQoSConditionVmSourceMacAddrStatus
  alaQoSConditionVmSourceMacMask
  alaQoSConditionVmSourceMacGroupId
  alaQoSConditionVmSourceMacGroupIdStatus
  alaQoSConditionVmSourceIpAddr
  alaQoSConditionVmSourceIpAddrStatus
  alaQoSConditionVmSourceIpMask
  alaQoSConditionVmSourceIpv6IpAddr
  alaQoSConditionVmSourceIpv6IpAddrStatus
  alaQoSConditionVmSourceIpv6IpMask
  alaQoSConditionVmIpProtocol
  alaQoSConditionVmIpProtocolStatus
  alaQoSConditionVmL4SourcePort
  alaQoSConditionVmL4SourcePortStatus
  alaQoSConditionVmL4DestPort
  alaQoSConditionVmL4DestPortStatus
  alaQoSConditionVxlanStatus
policy condition vxlan inner source mac

Configures a source MAC address as a policy condition for a VM Snooping policy rule. This type of condition applies to the source MAC address of the inner Ethernet frame of an encapsulated VXLAN packet.

`policy condition condition_name vxlan inner source mac mac_address [mask mac_mask]`

`policy condition condition_name vxlan no source mac`

Syntax Definitions

- **condition_name**: The name of an existing policy condition.
- **mac_address**: The source MAC address of a VM (inner MAC address of an encapsulated VXLAN frame).
- **mac_mask**: Optional. The mask for the source MAC address (for example, ff:ff:ff:ff:ff:ff).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of the command to remove the VM source MAC address from a condition; however, at least one classification parameter must be associated with a condition.
- The `vxlan` policy conditions are used to filter VXLAN packets received on VM Snooping ports.

Examples

```
-> policy condition c1 vxlan inner source mac 00:11:22:33:44:00
-> policy condition c2 vxlan inner source mac 00:20:da:05:f6:23 mask ff:ff:ff:ff:ff
-> policy condition c2 vxlan no source mac
```

Release History

Release 7.3.4; command was introduced.
Related Commands

qos apply
Applies configured QoS and policy settings to the current configuration.

policy condition vxlan
Creates a policy condition.

show policy condition
Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable

alaQoSConditionVmSourceMacAddr
alaQoSConditionVmSourceMacAddrStatus
alaQoSConditionVmSourceMacMask
**policy condition vxlan inner source mac-group**

Configures a source MAC address group as a policy condition for a VXLAN Snooping policy rule. This type of condition checks to see if the source MAC address of the inner Ethernet frame of an encapsulated VXLAN packet matches any of the MAC addresses specified in the MAC address group.

**Syntax**

`policy condition condition_name vxlan inner source mac-group group_name`

`policy condition condition_name vxlan no source mac-group`

**Syntax Definitions**

- `condition_name`: The name of an existing policy condition.
- `group_name`: The name of the source MAC group, configured through the `policy mac group` command.

**Defaults**

N/A.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove the source MAC address group name from a condition; however, at least one classification parameter must be associated with a condition.
- The `vxlan` policy conditions are used to filter packets received on VXLAN Snooping ports.

**Examples**

-> policy condition c1 vxlan inner source mac-group vm-macs
-> policy condition c1 vxlan no source mac-group

**Release History**

Release 7.3.4; command was introduced.
**Related Commands**

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **policy condition vxlan**  
  Creates a VXLAN policy condition.

- **show policy condition**  
  Shows information about policy conditions configured on the switch.

**MIB Objects**

alaQoSConditionTable

- alaQoSConditionVmSourceMacGroup
- alaQoSConditionVmSourceMacGroupStatus
policy condition vxlan inner source ip

Configures a source IPv4 address as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the source IP address of the inner Ethernet frame of an encapsulated VXLAN packet.

```
policy condition condition_name vxlan inner source ip ip_address [mask netmask]
policy condition condition_name vxlan no source ip
```

Syntax Definitions

- **condition_name**: The name of an existing policy condition.
- **ip_address**: A specific source IP address.
- **netmask**: The network mask for the source IP address (for example, 255.0.0.0, 255.255.0.0).

Defaults

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>netmask</td>
<td>IP address class</td>
</tr>
</tbody>
</table>
```

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of the command to remove the source IP address from a condition; however, at least one classification parameter must be associated with a condition.
- The **vxlan** policy conditions are used to filter VXLAN packets received on VXLAN Snooping ports.

Examples

- `-> policy condition c1 vxlan inner source ip 10.1.1.2`
- `-> policy condition c2 vxlan inner source ip 10.1.1.3 mask 255.0.0.0`
- `-> policy condition c1 vxlan no source ip`

Release History

Release 7.3.4; command was introduced.
Related Commands

- **qos apply**
  - Applies configured QoS and policy settings to the current configuration.

- **policy condition vxlan**
  - Creates a policy condition.

- **show policy condition**
  - Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  - alaQoSConditionVmSourceIpAddr
  - alaQoSConditionVmSourceIpAddrStatus
  - alaQoSConditionVmSourceIpMask
**policy condition vxlan inner source ipv6**

Configures a source IPv6 address as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the source IP address of the inner Ethernet frame of an encapsulated VXLAN packet.

```
policy condition condition_name vxlan inner source ipv6 ipv6_address [mask netmask]
policy condition condition_name vxlan no source ipv6
```

**Syntax Definitions**

- **condition_name**: The name of an existing policy condition.
- **ipv6_address**: A specific source IPv6 address.
- **netmask**: The network mask for the source IPv6 address.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>netmask</td>
<td>IPv6 address class</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove the source IPv6 address from a condition; however, at least one classification parameter must be associated with a condition.
- The `vxlan` policy conditions are used to filter VXLAN packets received on VXLAN Snooping ports.

**Examples**

- `-> policy condition c1 vxlan inner source ipv6 ::1234:531F:BCD2:F34A`
- `-> policy condition c1 vxlan no source ipv6`

**Release History**

Release 7.3.4; command was introduced.
Related Commands

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy condition vxlan**
  Creates a VXLAN Snooping policy condition.

- **show policy condition**
  Shows information about policy conditions configured on the switch.

MIB Objects

- **alaQoSConditionTable**
  - **alaQoSConditionVmSourceIpv6IpAddr**
  - **alaQoSConditionVmSourceIpv6IpAddrStatus**
  - **alaQoSConditionVmSourceIpv6IpMask**
**policy condition vxlan inner ip-protocol**

Configures a an IP protocol number as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the IP protocol of the inner Ethernet frame of an encapsulated VXLAN packet.

**policy condition condition_name vxlan inner ip-protocol protocol**

**policy condition condition_name vxlan no ip-protocol**

### Syntax Definitions

- **condition_name**: The name of an existing policy condition.
- **protocol**: The IP protocol number. The range is 0–255.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of the command to remove the IP protocol number from a condition; however, at least one classification parameter must be associated with a condition.

- The **vxlan** policy conditions are used to filter VXLAN packets received on VXLAN Snooping ports.

### Examples

- `-> policy condition c1 vxlan inner ip-protocol 6`
- `-> policy condition c1 vxlan no ip-protocol`

### Release History

Release 7.3.4; command was introduced.
Related Commands

qos apply  Applies configured QoS and policy settings to the current configuration.
policy condition vxlan  Creates a VXLAN Snooping policy condition.
show policy condition  Shows information about policy conditions configured on the switch.

MIB Objects

alaQoSConditionTable
  alaQoSConditionVmIpProtocol
  alaQoSConditionVmIpProtocolStatus
policy condition vxlan inner l4-port

Configures a Layer 4 (UDP or TCP) source port and/or destination port as a policy condition for a VXLAN Snooping policy rule. This type of condition applies to the Layer 4 port of the inner Ethernet frame of an encapsulated VXLAN packet.

```
policy condition condition_name vxlan inner l4-port {src src_port | dest dest_port}
policy condition condition_name vxlan no l4-port
```

**Syntax Definitions**

- `condition_name`: The name of an existing policy condition.
- `src_port`: The source port number. The valid range is 0–65535.
- `dest_port`: The destination port number. The valid range is 0–65535.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove the Layer 4 port number from a condition; however, at least one classification parameter must be associated with a condition.
- The `vxlan` policy conditions are used to filter packets received on VXLAN Snooping ports.

**Examples**

- `-> policy condition c1 vxlan inner l4-port dest 9445`
- `-> policy condition c1 vxlan inner l4-port src 4000`
- `-> policy condition c2 vxlan inner l4-port dest 8100 inner l4-port src 3000`
- `-> policy condition c1 vxlan no l4-port`

**Release History**

Release 7.3.4; command was introduced.
**Related Commands**

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.
- **policy condition vxlan**  
  Creates a VXLAN Snooping policy condition.
- **show policy condition**  
  Shows information about policy conditions configured on the switch.

**MIB Objects**

alaQoSConditionTable
  - alaQosConditionVmL4SourcePort
  - alaQosConditionVmL4SourcePortStatus
  - alaQosConditionVmL4DestPort
  - alaQosConditionVmL4DestPortStatus
policy condition vxlan vxlan-port

Configures a UDP destination port number as a policy condition for a VXLAN Snooping policy rule. This number is found in the outer IP header of an encapsulated VXLAN packet.

```
policy condition condition_name vxlan vxlan-port udp_port
policy condition condition_name vxlan no vxlan-port
```

### Syntax Definitions

- **condition_name**: The name of an existing policy condition.
- **udp_port**: The UDP destination port number of the VXLAN packet. The valid range is 0–65535

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove the VXLAN port number from a condition; however, at least one classification parameter must be associated with a condition.
- VXLAN packets use the well-known UDP destination port 4789 by default.
- The `vxlan` policy conditions are used to filter packets received on VXLAN Snooping ports.

### Examples

```
-> policy condition c1 vxlan vxlan-port 6000
-> policy condition c1 vxlan 7000
-> policy condition c1 vxlan no vxlan-port
```

### Release History

Release 7.3.4; command was introduced.
**Related Commands**

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.

- **policy condition vxlan**  
  Creates a VXLAN Snooping policy condition.

- **show policy condition**  
  Shows information about policy conditions configured on the switch.

**MIB Objects**

alaQoSConditionTable

- alaQoSConditionVxlanPort
- alaQoSConditionVxlanPortStatus
**policy action**

Configures or deletes a QoS action. A QoS action describes how traffic that matches a particular QoS condition should be treated. It may specify a particular set of bandwidth and queue parameters, or it may simply specify whether the flow is allowed or denied on the switch.

This section describes the base command. Optional keywords are listed below and described as separate commands later in this chapter. (Options may be used in combination but are described separately for ease in explanation.) Use the `no` form for keywords to remove the parameter from the action.

Note that some action parameters may not be supported depending on the platform you are using. Also some action parameters may not be supported with some conditions. See the condition in the *OmniSwitch AOS Release 8 Network Configuration Guide*.

```plaintext
policy action action_name
  [disposition {accept | drop | deny}]
  [shared]
  [priority priority_value]
  [maximum bandwidth bps]
  [maximum depth bytes]
  [cir bps [cbs bytes] [pir bps] [pbs bytes] [color-only]]
  [cpu priority priority]
  [tos tos_value]
  [802.1p 802.1p_value]
  [dscp dscp_value]
  [map {802.1p | tos | dscp} to {802.1p | tos | dscp} using map_group]
  [permanent gateway ip ip_address]
  [permanent gateway ipv6 ipv6_address]
  [port-disable]
  [redirect port chassis/slot/port]
  [redirect linkagg link_agg]
  [no-cache]
  [{ingress | egress | ingress egress | no} mirror {chassis/slot/port | session session_id}]
```

```plaintext
policy no action action_name
```

**Syntax Definitions**

- `action_name`  
  A name for the action, any alphanumeric string.

**Defaults**

By default, no drop algorithm is configured for the action, and any queues created by the action are not shared.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>drop</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Any condition parameters that the hardware supports will be used to classify the traffic; any condition parameters that are not supported by the hardware will not be used to classify traffic, and the event will be logged in the QoS log.
- Bandwidth parameters may be specified when the action is created or may be specified as separate commands.
- Use the `qos apply` command to activate configuration changes.
- Use the `no` form of the command to remove a QoS action from the configuration.
- If the `configuration snapshot` command is entered after the `policy action` command is configured, the resulting ASCII file will include the following additional syntax for the `policy action` command:

  ```
  from {cli | ldap | blt}
  ```

  This syntax indicates how the action was created. The `cli` and `ldap` options may be changed by a user modifying the ASCII file; however, changing this setting is not recommended. The `blt` option indicates a built-in action, this setting is not configurable.
- Policy action port-disable is not supported for service domain traffic.

Examples

```
-> policy action action1 accept
```

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; `session` keyword added.

Related Commands

- `policy condition`: Configures a condition associated with the action.
- `qos apply`: Applies configured QoS and policy settings to the current configuration.
- `show policy action`: Displays information about policy actions.

MIB Objects

- `alaQoSActionTable`
- `alaQoSActionName`
- `alaQoSActionSource`
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionSource
policy action disposition

Configures a disposition for a policy action.

policy action action_name disposition {accept | drop | deny}

Syntax Definitions

action_name  The name of the action.
accept       Specifies that the switch should accept the flow.
drop         Specifies that the switch should silently drop the flow.
deny         Specifies that the switch should drop the flow and issue an ICMP message indicating the flow was dropped for administrative reasons. Currently this option will provide the same result as drop; that is, the flow is silently dropped.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept</td>
<td>drop</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the no form of this command to remove a disposition from an action.

Examples

-> policy action a3 disposition deny

Release History

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**
  - Applies configured QoS and policy settings to the current configuration.
- **policy action**
  - Creates a policy action.
- **show policy action**
  - Displays information about policy actions.

MIB Objects

- **alaQoSActionTable**
  - **alaQoSActionName**
- **alaQoSActionDisposition**
- **alaQoSAppliedActionTable**
  - **alaQoSAppliedActionName**
  - **alaQoSAppliedActionDisposition**
**policy action shared**

Enables bandwidth sharing among multiple QoS rules that use the same maximum bandwidth action.

**policy action action\_name shared**

**policy action action\_name no shared**

### Syntax Definitions

<table>
<thead>
<tr>
<th>action_name</th>
<th>The name of the action.</th>
</tr>
</thead>
</table>

### Defaults

By default, queues created by an action are *not* shared.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If the *shared* policy action is not specified, then each bandwidth rule will implement a separate instance of the specified bandwidth allocation.
- Use the *no* form of the command to disable sharing.

### Example

- `-> policy action action5 maximum bandwidth 10m shared`
- `-> policy action action6 maximum bandwidth 10m shared`
- `-> policy action action5 no shared`

### Release History

Release 7.1.1; command was introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos apply</td>
<td>Applies configured QoS and policy settings to the current configuration.</td>
</tr>
<tr>
<td>policy action maximum</td>
<td>Creates a maximum bandwidth policy action.</td>
</tr>
<tr>
<td>bandwidth</td>
<td></td>
</tr>
<tr>
<td>show policy action</td>
<td>Displays information about policy actions.</td>
</tr>
</tbody>
</table>

### MIB Objects

- alaQoSActionTable
  - alaQoSActionName
  - alaQoSActionShared
- alaQoSAppliedActionTable
  - alaQoSAppliedActionName
  - alaQoSAppliedActionShared
policy action priority

Configures the priority for queuing a flow to which the QoS action applies.

policy action action_name priority priority_value

policy action action_name no priority

Syntax Definitions

action_name The name of the action.
priority_value The priority given to scheduling traffic on the output port. Values range from 0 (lowest) to 7 (highest).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove a priority value from an action.
- This priority value is independent of 802.1Q, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.

Examples

-> policy action action1 priority 1
-> policy action action1 no priority

Release History

Release 7.1.1; command was introduced.
Related Commands

qos apply
Applies configured QoS and policy settings to the current configuration.

policy action
Creates a policy action.

show policy action
Displays information about policy actions.

MIB Objects

alaQoSActionTable
  alaQoSActionName
  alaQoSActionPriority
  alaQoSActionPriorityStatus

alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionPriority
  alaQoSAppliedActionPriorityStatus
**policy action maximum bandwidth**

Configures a maximum bandwidth value for a policy action.

```
policy action action_name maximum bandwidth bps[k | m | g | t]
policy action action_name no maximum bandwidth
```

**Syntax Definitions**

- `action_name` The name of the action.
- `bps[k | m | g | t]` The maximum amount of bandwidth, in bits-per-second, for all traffic that ingress on the port. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k, 5m, 1g, 1t).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>k</td>
<td>m</td>
</tr>
<tr>
<td>k</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a maximum bandwidth value from an action.
- If the maximum bandwidth value is specified as an integer, without an abbreviated unit designation, the value is applied in kbps by default. For example, if the number 10 is specified, 10K is the maximum bandwidth value used. However, if 10G is specified, the maximum bandwidth value applied is 10 gbps.
- Use the `shared` policy action to enabling sharing of bandwidth across policy rules that specify the same maximum bandwidth action.

**Examples**

- `-> policy action action3 maximum bandwidth 10000`
- `-> policy action action4 maximum bandwidth 10k shared`
- `-> policy action action5 maximum bandwidth 10k shared`
- `-> policy action action4 no maximum bandwidth`
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **qos apply**  
  Applies configured QoS and policy settings to the current configuration.
- **policy action**  
  Creates a policy action.
- **show policy action**  
  Displays information about policy actions.

**MIB Objects**

- **alaQoSActionTable**
  - **alaQoSActionName**
  - **alaQoSActionMaximumBandwidth**
- **alaQoSAppliedActionTable**
  - **alaQoSAppliedActionName**
  - **alaQoSAppliedActionMaximumBandwidth**
**policy action maximum depth**

Configures the maximum queue depth or bucket size assigned to this action, in bytes. The queue depth or bucket size determines the amount of buffer allocated to each queue. When the queue depth or bucket size is reached, the switch starts dropping packets.

```
policy action action_name maximum depth bytes [K (kilo)| M (mega) | G (giga) | T (tera)]
policy action action_name no maximum depth
```

### Syntax Definitions

- **action_name**: The name of the action.
- **bytes [K | M | G | T]**: The maximum queue depth in bytes. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k, 5m, 1g). If the value is entered as an integer, the switch uses the default unit of K(kilo).

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>M</td>
</tr>
<tr>
<td>bytes</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove a maximum depth value from a policy action.
- If the maximum depth value is specified as an integer, without an abbreviated unit designation, the value is applied in Kbytes by default. For example, if the number 10 is specified, 10K bytes is the maximum depth value used. However, if 10G is specified, the maximum depth value applied is 10G bytes.
- A maximum depth action is used in combination with a maximum bandwidth action.

### Examples

```
-> policy action action2 maximum depth 100
-> policy action action2 no maximum depth
```
Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply  Applies configured QoS and policy settings to the current configuration.
policy action  Creates a policy action.
show policy action  Displays information about policy actions.

MIB Objects

alaQoSActionTable
  alaQoSActionName
  alaQoSActionMaximumDepth
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionMaximumDepth
**policy action cir**

Configures a Tri-Color Marking (TCM) policy action. This type of action includes parameters for Committed Information Rate (CIR), Committed Burst Size (CBS), Peak Information Rate (PIR), and Peak Burst Size (PBS). The TCM policier meters and marks packets red, green, or yellow based on the parameter values of this policy action.

```
policy action action_name cir bps [cbs bytes] [pir bps] [pbs bytes] [color-only]
policy action action_name no cir
policy action action_name no pir
```

### Syntax Definitions

- **action_name**
  - The name of the action.

- **bps [k | m | g | t]**
  - The maximum amount of bandwidth, in bits-per-second, for all traffic that ingresses on the port. The value may be entered as an integer (for example, `10`) or with abbreviated units (for example, `10k, 5m, 1g, 1t`).

- **bytes**
  - The desired value for maximum bucket size, in bytes.

- **color-only**
  - Disables TCM rate limiting based on the metering results. Packets are only marked the specific color that applies to the level of packet conformance.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cir pir bps</td>
<td>0</td>
</tr>
<tr>
<td>cbs pbs bytes</td>
<td>10K</td>
</tr>
<tr>
<td>k</td>
<td>m</td>
</tr>
</tbody>
</table>

By default, this action enables rate limiting based on TCM marking and metering.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the TCM parameter values.
• If the **color-only** parameter is specified with this command, the TCM action will only mark packet color; packets are not rate limited based on the metering results. In this case, packets are then subject to any rate limiting specifications as defined in the queue management configuration for the switch.

• This implementation of TCM supports two rate limiting modes: Single-Rate (srTCM) and Two-Rate (trTCM). The srTCM mode marks packets based only on the CIR and the two burst sizes: CBS and PBS. The trTCM mode marks packets based on both the CIR and PIR and their associated CBS and PBS values.

• There is no explicit CLI command to configure the mode (srTCM or trTCM) in which the TCM meter operates. Instead, the mode is determined by the CIR and PIR values configured for the policy action. If the PIR value is greater than the CIR value, trTCM is used. If the PIR value is less than the CIR value, srTCM is used.

• Configuring CIR and CBS is similar to configuring a maximum bandwidth. Configuring CIR and PIR is similar to configuring maximum depth.

• The number of packets counted as a result of the counter color mode setting is displayed using the **show active policy rule** command. These statistics are only shown for those rules that are configured with a TCM policy action.

**Examples**

The following command examples configure srTCM (the default):

```bash
-> policy action A3 cir 10M
-> policy action A4 cir 10M cbs 4k
-> policy action A5 cir 10M cbs 4k pir 10M
-> policy action A6 cir 10M cbs 4k pir 10M pbs 4k
-> policy action a7 cir 5M cbs 2k color-only
-> policy action A3 no cir
-> policy action A5 no pir
```

The following command examples configure trTCM (note that PIR is greater than CIR):

```bash
-> policy action A7 cir 10M cbs 4k pir 20M
-> policy action A8 cir 10M cbs 4k pir 20M pbs 40M
-> policy action a9 cir 5M cbs 1M pbs 10M pbs 2M color-only
-> policy action A7 no cir
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy action**
  Creates a policy action.

- **show policy action**
  Displays information about policy actions.
**MIB Objects**

alaQoSActionTable
  alaQoSActionCIR
  alaQoSActionCIRStatus
  alaQoSActionCBS
  alaQoSActionCBSStatus
  alaQoSActionPIR
  alaQoSActionPIRStatus
  alaQoSActionPBS
  alaQoSActionPBSStatus
  alaQoSActionColorOnly

alaQoSAppliedActionTable
  alaQoSAppliedActionCIR
  alaQoSAppliedActionCIRStatus
  alaQoSAppliedActionCBS
  alaQoSAppliedActionCBSStatus
  alaQoSAppliedActionPIR
  alaQoSAppliedActionPIRStatus
  alaQoSAppliedActionPBS
  alaQoSAppliedActionPBSStatus
  alaQoSAppliedColorOnly
policy action cpu priority

Configures a CPU priority policy action.

policy action action_name cpu priority priority

policy action action_name no cpu priority

Syntax Definitions

action_name
The name of the action.

priority
The CPU queue on which packets destined for the CPU are received.
The valid range is 0–31.

Defaults

By default, the CPU priority is set to zero.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the no form of this command to remove the CPU priority parameter value.

Examples

- -> policy action A7 cpu priority 15
- -> policy action A8 cpu priority 31
- -> policy action A7 no cpu priority

Release History

Release 7.1.1; command was introduced.
Related Commands

qos apply
Applies configured QoS and policy settings to the current configuration.

policy action
Creates a policy action.

show policy action
Displays information about policy actions.

MIB Objects
alaQoSActionTable
alaQoSActionCPUPriority
alaQoSActionCPUPriorityStatus
alaQoSAppliedActionTable
alaQoSAppliedActionCPUPriority
alaQoSAppliedActionCPUPriorityStatus
**policy action tos**

Configures a Type of Service (ToS) bits value to be applied to packets in outgoing flows to which the specified policy applies.

```
policy action action_name tos tos_value
policy action action_name no tos
```

**Syntax Definitions**

*action_name*  
The name of the action.

*tos_value*  
The three-bit priority value in the IP header that should be set on outgoing frames in flows that match the specified policy. Values range from 0 (lowest priority) to 7 (highest priority).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the no form of this command to remove a ToS value from a policy action.
- Note that specifying both ToS and DSCP in the same action is not allowed.

**Examples**

```
-> policy action action3 tos 4
-> policy action action3 no tos
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.
- **policy action**
  Creates a policy action.
- **show policy action**
  Displays information about policy actions.

MIB Objects

- **alaQoSActionTable**
  - **alaQoSActionName**
  - **alaQoSActionTos**
- **alaQoSAppliedActionTable**
  - **alaQoSAppliedActionName**
  - **alaQoSAppliedActionTos**
**policy action 802.1p**

Configures a value to be set in the 802.1p bits of the 802.1Q byte of an outgoing frame for traffic that matches a policy with this action.

**policy action action_name 802.1p 802.1p_value**

**policy action action_name no 802.1p**

**Syntax Definitions**

- **action_name**: The name of the action.
- **802.1p_value**: The priority value to be set in 802.1Q frames. Values range from 0 (lowest priority) to 7 (highest priority).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove an 802.1p value from a policy action.
- Note that specifying both ToS and DSCP in the same action is not allowed.

**Examples**

- `-> policy action action4 802.1p 7`
- `-> policy action action4 no 802.1p`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- qos apply: Applies configured QoS and policy settings to the current configuration.
- policy action: Creates a policy action.
- show policy action: Displays information about policy actions.

MIB Objects

alaQoSActionTable
  alaQoSActionName
  alaQoSAction8021p
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedAction8021p
**policy action dscp**

Configures a Differentiated Services Code Point (DSCP) value to be set in an outgoing flow for traffic that matches rules with this action.

`policy action action_name dscp dscp_value`

`policy action action_name no dscp`

---

**Syntax Definitions**

- **action_name**
  - The name of the action.

- **dscp_value**
  - The DSCP value to be set, in the range 0–63.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a DSCP value from a policy action.
- Note that specifying both ToS and DSCP in the same action is **not** allowed.

**Examples**

```bash
-> policy action action2 dscp 61
-> policy action action2 no dscp
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy action**
  Creates a policy action.

- **show policy action**
  Displays information about policy actions.

MIB Objects

- **alaQoSActionTable**
  - **alaQoSActionName**
  - **alaQoSActionDscp**

- **alaQoSAppliedActionTable**
  - **alaQoSAppliedActionName**
  - **alaQoSAppliedActionDscp**
policy action map

Configures a mapping group for a policy action.

policy action map {802.1p | tos | dscp} to {802.1p | tos | dscp} using map_group

policy action no map

Syntax Definitions

action_name The name of the action.
802.1p Indicates that an 802.1p value should be mapped.
tos Indicates that a ToS value should be mapped.
dscp Indicates that a DSCP value should be mapped.
map_group The name of the map group, configured through the policy map group command.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/C32E</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C8/V48C8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- When remapping is configured with this command and a flow matches a policy with this remapping action, and the 802.1p, ToS, or DSCP setting in the incoming flow is specified by the map group, the value will be remapped in the outgoing flow according to the map group.
- If the 802.1p, ToS, or DSCP setting in the incoming flow is not a value specified in the map group, the switch will do one of two things:
  - If the remap from and remap to types are the same (802.1p to 802.1p, ToS to ToS, or DSCP to DSCP), the values in the outgoing flow will be unchanged. If the remap from and remap to types are not the same (for example: 802.1p to ToS), the switch will determine the outgoing 802.1p and ToS based on whether or not the port is trusted or untrusted.
- Use the no form of the command to delete the map group from the configuration.

Examples

- policy action a1 map 802.1p to 802.1p using mapGroup2
- policy action a2 map 802.1p to tos using mapGroup3
Release History

Release 7.1.1; command was introduced.

Related Commands

- **policy map group**
  Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.

- **qos apply**
  Applies configured QoS and policy settings to the current configuration.

- **policy action**
  Creates a policy action.

- **show policy action**
  Displays information about policy actions.

- **show policy map group**
  Displays information about all pending and applied policy map groups or a particular map group.

MIB Objects

alaQoSActionTable
- alaQoSActionMapFrom
- alaQoSActionMapTo
- alaQoSActionMapGroup

alaQoSAppliedActionTable
- alaQoSAppliedActionMapFrom
- alaQoSAppliedActionMapToalaQoSAppliedActionMapGroup
policy action permanent gateway-ip

Used for Policy Based Routing (PBR). Routed flows to which this action is applied will be directed to the IP address specified in the action regardless of whether or not a route already exists in the switch routing table.

\[ \text{policy action } action\_name \text{ permanent gateway-ip } ip\_address \]

\[ \text{policy action } action\_name \text{ no permanent gateway-ip } \]

**Syntax Definitions**

- action_name: The name of the action.
- ip_address: The destination IP address to which packets will be routed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a gateway IP address from a policy action.
- If the gateway goes down, the traffic to be routed over the gateway will be dropped.

**Examples**

- `-> policy action pbr2 permanent gateway-ip 10.10.2.1`
- `-> policy action pbr2 no permanent gateway-ip`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

qos apply
Applies configured QoS and policy settings to the current configuration.

policy action
Creates a policy action.

show policy action
Displays information about policy actions.

MIB Objects

alaQoSActionTable
alaQoSActionName
alaQoSActionPermanentGatewayIpAddr
alaQoSAppliedActionTable
alaQoSAppliedActionName
alaQoSAppliedActionPermanentGatewayIpAddr
**policy action permanent gateway-ipv6**

Used for Policy Based Routing (PBR). Routed flows to which this action is applied will be directed to the IPv6 address specified in the action regardless of whether or not a route already exists in the switch routing table.

```
policy action action_name permanent gateway-ipv6 ipv6_address

policy action action_name no permanent gateway-ipv6
```

---

**Syntax Definitions**

- `action_name`  
The name of the action.
- `ipv6_address`  
The destination IPv6 address to which packets will be routed.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of the command to remove a gateway IPv6 address from a policy action.
- If the gateway goes down, the traffic to be routed over the gateway will be dropped.

---

**Examples**

- `-> policy action pbr2 permanent gateway-ipv6 2607:f0d0:2001:000a:0000:0000:0010`
- `-> policy action pbr2 no permanent gateway-ipv6`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

qos apply  Applies configured QoS and policy settings to the current configuration.
policy action  Creates a policy action.
show policy action  Displays information about policy actions.

MIB Objects

alaQoSActionTable
alaQoSActionName
alaQoSActionPermanentGatewayIpV6Addr
alaQoSAppliedActionTable
alaQoSAppliedActionName
alaQoSAppliedActionPermanentGatewayIpV6Addr
**policy action port-disable**

Administratively disables the source port of the traffic to which this action is applied.

`policy action action_name port-disable`

`policy action action_name no port-disable`

---

**Syntax Definitions**

*action_name*  
The name of the action.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the *no* form of this command to remove *port-disable* from the policy action.
- An SNMP trap is sent when a port is administratively disabled through a port disable action or a UserPorts shutdown function.
- To enable a port disabled by this action, use the *interfaces* or *interfaces port break-out* command to administratively enable the port, or physically disconnect and reconnect the port cable.

---

**Examples**

- `-> policy action pd01 port-disable`
- `-> policy action pb02 no port-disable`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy action**: Creates a policy action.
- **show policy action**: Displays information about policy actions.
- **interfaces**: Administratively enables or disables a port.
- **interfaces wait-to-restore**: Administratively clears the violation that disabled the port or link aggregate and restores the port to enabled status.

MIB Objects

- **alaQoSActionTable**
  - **alaQoSActionName**
  - **alaQoSActionPortdisable**
- **alaQoSAppliedActionTable**
  - **alaQoSAppliedActionName**
  - **alaQoSAppliedActionPortdisable**
policy action redirect port

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified port instead of the port to which the traffic was destined.

policy action action_name redirect port chassis/slot/port

policy action action_name no redirect port

**Syntax Definitions**

- **action_name**: The name of the action.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number that will receive the redirected traffic.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of the command to remove **redirect port** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect port must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect port is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified port or link aggregate and is “blackholed”. As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will **not** trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port must belong to VLAN A (tagged or default VLAN).
Examples

-> policy action rp01 redirect port 1/12/1
-> policy action rp01 no redirect port

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply
   Applies configured QoS and policy settings to the current configuration.
policy action
   Creates a policy action.
show policy action
   Displays information about policy actions.

MIB Objects

alaQoSActionTable
   alaQoSActionName
   alaQoSActionRedirectSlot
   alaQoSActionRedirectPort
alaQoSAppliedActionTable
   alaQoSAppliedActionName
   alaQoSAppliedActionRedirectSlot
   alaQoSAppliedActionRedirectPort
policy action redirect linkagg

Redirects all traffic (flooded, bridged, routed, and multicast) matching a redirect policy to the specified link aggregate ID instead of the link aggregate to which the traffic was destined.

\[ \text{policy action action\_name redirect linkagg agg\_id} \]

\[ \text{policy action action\_name no redirect linkagg} \]

**Syntax Definitions**

- **action\_name**: The name of the action.
- **agg\_id**: The link aggregate ID number (0–32) to assign to the specified VLAN. See the “Link Aggregation Commands” chapter in this guide.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove **redirect linkagg** from the policy action.
- When redirecting routed traffic from VLAN A to VLAN B, the redirect link aggregate ID must belong to VLAN B (tagged or default VLAN).
- Routed packets (from VLAN A to VLAN B) are not modified after they are redirected; the source and MAC address remain the same. In addition, if the redirect link aggregate ID is tagged, the redirected packets will have a tag from the ingress VLAN A.
- If a route exists for the redirected flow, then redirected packets are the final post-routing packets.
- If a route does not exist for the redirected flow, the flow is not redirected to the specified link aggregate ID and is “blackholed”. As soon as a route is available, the flow is then redirected as specified in the policy.
- In most cases, a redirected flow will **not** trigger an update to the routing and ARP tables. If necessary, create a static route for the flow or assign the redirect port or link aggregate ID to the ingress VLAN (VLAN A) to send packets to the redirect port until a route is available.
- When redirecting bridged traffic on VLAN A, the redirect port or link aggregate ID must belong to VLAN A (tagged or default VLAN).
Examples

-> policy action rp01 redirect linkagg 2
-> policy action rp01 no redirect linkagg 2

Release History

Release 7.1.1; command was introduced.

Related Commands

qos apply
Applies configured QoS and policy settings to the current configuration.
policy action
Creates a policy action.
show policy action
Displays information about policy actions.

MIB Objects

alaQoSActionTable
  alaQoSActionName
  alaQoSActionRedirectAgg
alaQoSAppliedActionTable
  alaQoSAppliedActionName
  alaQoSAppliedActionRedirectAgg
**policy action no-cache**

Disables logging of rule entries to the hardware cache.

```plaintext
policy action action_name no-cache
```

```plaintext
policy action action_name no no-cache
```

---

**Syntax Definitions**

`action_name`  
The name of the action.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to remove `no-cache` from the policy action.
- Recommended for use when applied to traffic going to the switch.

---

**Examples**

- `-> policy action nc01 no-cache`
- `-> policy action nc01 no no-cache`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **qos apply**: Applies configured QoS and policy settings to the current configuration.
- **policy action**: Creates a policy action.
- **show policy action**: Displays information about policy actions.

MIB Objects

- `alaQoSActionTable`
  - `alaQoSActionName`
  - `alaQoSActionNocache`
- `alaQoSAppliedActionTable`
  - `alaQoSAppliedActionName`
  - `alaQoSAppliedActionNocache`
**policy action mirror**

Mirrors ingress, egress, or both ingress and egress packets that match a mirroring policy to the specified port.

```
policy action action_name [ingress | egress | ingress egress] mirror {chassis/slot/port | session session_id}

policy action action_name no mirror {chassis/slot/port | session session_id}
```

### Syntax Definitions

- **action_name**
  - The name of the action.

- **ingress**
  - Mirrors ingress packets.

- **egress**
  - Mirrors egress packets.

- **ingress egress**
  - Mirrors ingress and egress packets.

- **chassis**
  - The chassis identifier.

- **slot/port**
  - The slot and port number that will receive the mirrored traffic.

- **session_id**
  - Mirroring session identifier. This parameter is supported only on the OmniSwitch 9900.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ingress</td>
<td>ingress</td>
</tr>
<tr>
<td>egress</td>
<td>ingress</td>
</tr>
<tr>
<td>ingress egress</td>
<td>ingress</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove `mirror` from the policy action.

- Use this command to configure a mirror-to-port (MTP) and mirror-to-session action used for policy based mirroring.

- Only one policy-based MTP session is supported at any given time either port-based policy mirroring or session-based policy mirroring. As a result, all mirroring policies must specify the same destination port or same port mirroring session ID.

- Policy based mirroring and the port based mirroring feature can run simultaneously on the same switch.
**Examples**

-> policy action a1 mirror 1/7/1 (default ingress)
-> policy action a1 ingress mirror 1/7/1
-> policy action a1 egress mirror 1/7/1
-> policy action a1 ingress egress mirror 1/7/1
-> policy action a1 no mirror
-> policy action a1 mirror session 1

**Release History**

Release 7.1.1; command was introduced.
Release 8.6R1; session keyword introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>qos apply</code></td>
<td>Applies configured QoS and policy settings to the current configuration.</td>
</tr>
<tr>
<td><code>policy action</code></td>
<td>Creates a policy action.</td>
</tr>
<tr>
<td><code>show policy action</code></td>
<td>Displays information about policy actions.</td>
</tr>
</tbody>
</table>

**MIB Objects**

alaQoSActionTable
  alaQoSActionName
  alaQoSActionMirrorSlot
  alaQosActionMirrorPort
  alaQosActionMirrorMode
  alaQosActionMirrorModeStatus
**show policy network group**

Displays information about pending and applied policy network groups.

```
show [applied] policy network group [network_group]
```

---

### Syntax Definitions

- **applied**
  - Displays only network groups that have been applied.

- **network_group**
  - The name of the policy network group for which you want to display information; or a wildcard sequence of characters for displaying information about network groups with similar names. Use an asterisk (*) to indicate a wildcard character.

---

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Information for all policy network groups displays unless `network_group` is specified.

### Examples

```
-> show policy network group
Group Name                       : netg1
 State                          = new,
 Entries                        = 198.206.10.1

-> show policy network group
Group Name                       : group1
 Entires                        = 203.185.129.0 mask 255.255.255.0, 203.185.131.192 mask 255.255.255.192, 203.185.132.0 mask 255.255.252.0, 204.226.0.0 mask 255.255.0.0
```
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the port group, configured through the <code>policy network group</code> command.</td>
</tr>
<tr>
<td>State</td>
<td>This field appears if the group was created or modified but not yet applied to the QoS configuration. When the <code>qos apply</code> command is issued, this field no longer displays.</td>
</tr>
<tr>
<td>Entries</td>
<td>The IP addresses associated with the network group.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `policy network group`: Configures policy network groups.

**MIB Objects**

- `alaQoSNetworkGroupsTable`
  - `alaNetworkGroupsName`
  - `alaNetworkGroupsSource`
- `alaNetworkGroupTable`
  - `alaNetworkGroupIpAddr`
  - `alaQoSNetworkGroupIpMask`
**show policy service**

Displays information about pending and applied policy services.

```
show [applied] policy service [service_name]
```

### Syntax Definitions

- **applied**
  - Displays only policy services that have been applied.

- **service_name**
  - The name of the service for which you want to display information; or a wildcard sequence of characters for displaying information about services with similar names. Use an asterisk (*) to indicate a wildcard character.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Information about all policy services is displayed unless `service_name` is specified.

### Examples

```
-> show policy service
Service name : sl
  State       = new,
  Destination UDP port = 1001-2004
```

### Output definitions

- **Service Name**
  - The name of the port group, configured through the `policy service` command.

- **State**
  - This field appears if the service was created or modified but not yet applied to the QoS configuration. When the `qos apply` command is issued, this field no longer displays.

- **IPProto**
  - The IP protocol associated with the service.

- **ScrPort**
  - A source port associated with the service.

- **DstPort**
  - A destination port associated with the service.
Release History

Release 7.1.1; command was introduced.

Related Commands

policy service

Configures a service that may be used as part of a policy service group.

MIB Objects

alaQoSServiceTable
  alaQoSGetName
  alaQoSGetServiceSource
  alaQoSGetServiceIpProtocol
  alaQoSGetServiceSourceIpPort
  alaQoSGetServiceDestinationIpPort
alaQoSAppliedServiceTable
  alaQoSAppliedServiceName
  alaQoSAppliedServiceSource
  alaQoSAppliedServiceIpProtocol
  alaQoSAppliedSourceIpPort
  alaQoSAppliedServiceDestinationIpPort
**show policy service group**

Displays information about pending and applied policy service groups.

```
show [applied] policy service group [service_group]
```

**Syntax Definitions**

- **applied**
  - Displays only policy service groups that have been applied.

- **service_group**
  - The name of the service group for which you want to display information; or a wildcard sequence of characters for displaying information about service groups with similar names. Use an asterisk (*) to indicate a wildcard character.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Information for all policy service groups displays unless `service_group` is specified.

**Examples**

```
-> show policy service group
Group Name    : mgmt
  State        : new,
  Entries      : ftp,
                http,
                https,
                snmp,
                ssh,
                telnet
```

**output definitions**

- **Group Name**
  - The name of the port group, configured through the `policy service group` command.
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>This field appears if the group was created or modified but not yet applied to the QoS configuration. When the <code>qos apply</code> command is issued, this field no longer displays.</td>
</tr>
<tr>
<td>Entries</td>
<td>The services associated with the group. Services are configured through the <code>policy service</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**policy service group**

Configures a service group and its associated services. A service group may be attached to a policy condition.

**MIB Objects**

- `alaQoSServiceGroupsTable`  
  - `alaQoSServiceGroupsName`  
  - `alaQoSServiceGroupsSource`

- `alaQoSAppliedServiceGroupsTable`
  - `alaQoSAppliedServiceGroupsName`
  - `alaQoSAppliedServiceGroupsSource`

- `alaQoSServiceGroupTable`
  - `alaQoSServiceGroupServiceName`

- `alaQoSAppliedServiceGroupTable`
  - `alaQoSAppliedServiceGroupServiceName`
**show policy mac group**

Displays information about pending and applied MAC groups.

```
show [applied] policy mac group [mac_group]
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applied</td>
<td>Displays only MAC groups that have been applied.</td>
</tr>
<tr>
<td>mac_group</td>
<td>The name of the MAC group for which you want to display information; or a wildcard sequence of characters for displaying information about MAC groups with similar names. Use an asterisk (*) to indicate a wildcard character.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Information for all policy MAC groups displays unless `mac_group` is specified.

**Examples**

```
-> show policy mac group
Group Name             : mgl
  State                = new,
  Entries             = 00:02:9A:44:5E:10 mask 00:00:00:FF:FF:FF,
                        00:11:01:00:00:01 mask 00:00:00:FF:FF:FF
                        00:02:9A:44:5E:20
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the port group, configured through the <code>policy mac group</code> command.</td>
</tr>
<tr>
<td>State</td>
<td>This field appears if the group was created or modified but not yet applied to the QoS configuration. When the <code>qos apply</code> command is issued, this field no longer displays.</td>
</tr>
<tr>
<td>Entries</td>
<td>The MAC addresses associated with the group.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **policy mac group** Configures policy MAC groups.

**MIB Objects**

- `alaQoSMACGroupsTable`
  - `alaQoSMACGroupsName`
  - `alaQoSMACGroupsSource`
- `alaQoSAppliedMACGroupsTable`
  - `alaQoSAppliedMACGroupsName`
  - `alaQoSAppliedMACGroupsSource`
- `alaQoSMACGroupTable`
  - `alaQoSMACGroupMacAddr`
  - `alaQoSMACGroupMacMask`
- `alaQoSAppliedMACGroupTable`
  - `alaQoSAppliedMACGroupMacAddr`
  - `alaQoSAppliedMACGroupMacMask`
**show policy port group**

Displays information about pending and applied policy port groups.

```
show [applied] policy port group [group_name]
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applied</td>
<td>Displays only policy port groups that have been applied.</td>
</tr>
<tr>
<td>group_name</td>
<td>The name of the policy port group for which you want to display information; or a wildcard sequence of characters for displaying information about port groups with similar names. Use an asterisk (*) to indicate a wildcard character.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platform</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Information for all policy port groups displays unless `group_name` is specified.

**Examples**

```
-> show policy port group
Group Name       : pg1
    State       = new,
    Entries     = 1/2/1,
                  1/3/1,
                  1/4/1,
                  3/1/11
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the port group, configured through the <code>policy port group</code> command or built-in port groups automatically set up by the switch (Slot01, Slot02, Slot03, etc.).</td>
</tr>
<tr>
<td>State</td>
<td>This field appears if the group was created or modified but not yet applied to the QoS configuration. When the <code>qos apply</code> command is issued, this field no longer displays.</td>
</tr>
<tr>
<td>Entries</td>
<td>The slot/port combinations associated with the port group.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **policy port group**
  Configures a port group and its associated slot and port numbers.

**MIB Objects**

- `alaQoSPortGroupsTable`
  - `alaQoSPortGroupsName`
  - `alaQoSPortGroupsSource`
- `alaQoSAppliedPortGroupsTable`
  - `alaQoSAppliedPortGroupsName`
  - `alaQoSAppliedPortGroupsSource`
- `alaPortGroupTable`
  - `alaQoSPortGroupSlot`
  - `alaQoSPortGroupPort`
- `alaAppliedPortGroupTable`
  - `alaQoSAppliedPortGroupSlot`
  - `alaQoSAppliedPortGroupPort`
show policy map group

Displays information about pending and applied policy map groups.

**show [applied] policy map group [group_name]**

**Syntax Definitions**

<table>
<thead>
<tr>
<th>applied</th>
<th>Displays only policy map groups that have been applied.</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_name</td>
<td>The name of the policy map group for which you want to display information; or a wildcard sequence of characters for displaying information about map groups with similar names. Use an asterisk (*) to indicate a wildcard character.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Information for all policy map groups displays unless *group_name* is specified.

**Examples**

-> show policy map group
Group Name : ml
  State     = new,
  Entries   = 0:0,
            1:9,
            2:18,
            3:27,
            4:36,
            5:45,
            6:54,
            7:63
output definitions

<table>
<thead>
<tr>
<th>Group Name</th>
<th>The name of the map group, configured through the <code>policy map group</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>This field appears if the group was created or modified but not yet applied to the QoS configuration. When the <code>qos apply</code> command is issued, this field no longer displays.</td>
</tr>
<tr>
<td>Entries</td>
<td>The slot/port combinations associated with the port group.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

`policy map group` Configures a map group and its associated mappings for 802.1p, Type of Service (ToS), or Differentiated Services Code Point (DSCP) values.

MIB Objects

alaQoSMapGroupsTable
  alaQoSMapGroupsName
  alaQoSMapGroupsSource
alaQoSAppliedMapGroupsTable
  alaQoSAppliedMapGroupsName
  alaQoSAppliedMapGroupsSource
alaQoSMapGroupTable
  alaQoSMapGroupKey
  alaQoSMapGroupKeyEnd
  alaQoSMapGroupValue
alaQoSAppliedMapGroupTable
  alaQoSAppliedMapGroupKey
  alaQoSAppliedMapGroupKeyEnd
  alaQoSAppliedMapGroupValue
show policy action

Displays information about pending and applied policy actions configured on the switch.

show [applied] policy action [action_name]

Syntax Definitions

applied  Displays only actions that have been applied to the QoS configuration for the switch.

action_name  The name of the action for which you want to display information; or a wildcard sequence of characters for displaying information about actions with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Information for all policy actions displays unless action_name is specified.
- When the optional applied parameter is used, pending QoS actions are not displayed.

Examples

-> show policy action
Action name  : a1
  Committed Information Rate = 10.0M,
  Committed Burst size      = 5.00M,
  Peak Information Rate     = 20.0M,
  Peak Burst size           = 5.00M

Action name  : a2
  State            = new,
  Disposition      = deny

Action name  : a3
  State            = new,
  Priority         = 7,
show applied policy action

Action name: a1
Commited Information Rate = 10.0M,
Commited Burst size = 5.00M,
Peak Information Rate = 20.0M,
Peak Burst size = 5.00M

<table>
<thead>
<tr>
<th>Action Name</th>
<th>The name of the action, configured through the <strong>policy action</strong> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>This field appears if the action was created or modified but not yet applied to the QoS configuration. When the <strong>qos apply</strong> command is issued, this field no longer displays.</td>
</tr>
<tr>
<td>Policy Action Parameters</td>
<td>Displays the configured policy action parameters.</td>
</tr>
</tbody>
</table>

**Release History**
Release 7.1.1; command was introduced.

**Related Commands**

**policy action**
Creates a policy action. A QoS action is a particular set of bandwidth and queue parameters that may be applied to a flow matching particular QoS conditions.

**MIB Objects**

alaQoSActionTable
  - alaQoSActionName
  - alaQoSActionSource
  - alaQoSActionDisposition
  - alaQoSActionShared
  - alaQoSActionMinimumBandwidth
  - alaQoSActionMaximumBandwidth
  - alaQoSActionMaximumDepth

alaQoSAppliedActionTable
  - alaQoSAppliedActionName
  - alaQoSAppliedActionSource
  - alaQoSAppliedActionDisposition
  - alaQoSAppliedActionShared
  - alaQoSAppliedActionMinimumBandwidth
  - alaQoSAppliedActionMaximumBandwidth
  - alaQoSAppliedActionMaximumDepth
show policy condition

Displays information about pending and applied policy conditions.

```
show [applied] policy condition [condition_name]
```

**Syntax Definitions**

- **applied**
  - Displays only conditions that have been applied to the QoS configuration for the switch.

- **condition_name**
  - The name of the condition for which you want to display information; or a wildcard sequence of characters for displaying information about actions with similar names. Use an asterisk (*) to indicate a wildcard character.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Information for all policy conditions displays unless `condition_name` is specified.
- When the optional `applied` parameter is used, pending QoS conditions are not displayed.

**Examples**

```
-> show policy condition
Condition name : c1
   Source VLAN  = 1001

Condition name : c2
   State       = new,
   Source IP   = 10.2.2.1,
   Destination UDP port = 17

-> show applied policy condition
Condition name : c1
   Source VLAN  = 1001
```
show policy condition

- Condition name: c1
- Application group = apg1

- Condition name: c2
- State = new,
- Application name = "jabber -init sequence",
- Destination UDP port = 17

**output definitions**

<table>
<thead>
<tr>
<th>Condition Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the condition, configured through the <strong>policy condition</strong> command.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field appears if the condition was created or modified but not yet applied to the QoS configuration. When the <strong>qos apply</strong> command is issued, this field no longer displays.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source VLAN</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The source VLAN.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination UDP port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The destination UDP port.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the AppMon application group to which the QoS policy condition is applied.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the AppMon application to which the QoS policy condition applied.</td>
<td></td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**policy condition**

Creates a policy condition. The condition determines what parameters the switch uses to classify incoming flows.
**MIB Objects**

alaQoSConditionTable
  
  alaQoSConditionName
  alaQoSConditionSource
  alaQoSConditionSourceSlot
  alaQoSConditionSourcePort
  alaQoSConditionSourcePortGroup
  alaQoSConditionDestinationSlot
  alaQoSConditionDestinationPort
  alaQoSConditionDestinationPortGroup
  alaQoSConditionSourceInterfaceType
  alaQoSConditionDestinationInterfaceType
  alaQoSConditionSourceMacAddr
  alaQoSConditionSourceMacMask
  alaQoSConditionSourceMacGroup
  alaQoSConditionDestinationMacAddr
  alaQoSConditionDestinationMacMask
  alaQoSConditionDestinationMacGroup
  alaQoSConditionSourceVlan
  alaQoSConditionDestinationVlan
  alaQoSCondition8021p
  alaQoSConditionSourceIpAddr
  alaQoSConditionSourceIpMask
  alaQoSConditionSourceNetworkGroup
  alaQoSConditionDestinationIpAddr
  alaQoSConditionDestinationIpMask
  alaQoSConditionDestinationNetworkGroup
  alaQoSConditionMulticastIpAddr
  alaQoSConditionMulticastIpMask
  alaQoSConditionMulticastNetworkGroup
  alaQoSConditionTos
  alaQoSConditionDscp
  alaQoSConditionTcpFlags
  alaQoSConditionIpProtocol
  alaQoSConditionSourceIpPort
  alaQoSConditionDestinationIpPort
  alaQoSConditionService
  alaQoSConditionServiceGroup
show active policy rule

Displays information about pending and applied policy rules that are active (enabled) on the switch.

`show active policy rule [rule_name]`

**Syntax Definitions**

`rule_name`  
The name of the rule for which you want to display information; or a wildcard sequence of characters for displaying information about rules with similar names. Use an asterisk (*) to indicate a wildcard character.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `show policy rule` command to display inactive as well as active policy rules.
- Information for all rules is displayed unless `rule_name` is specified.
- Applied rules may or may not be active on the switch. Applied rules are inactive if they have been administratively disabled with the `disable` option in the `policy rule` command.

**Examples**

```
-> show active policy rule
Rule name    : rl
  Condition name = c1,
  Action name    = a1,
  Packets        = 4166772,
  Bytes          = 266665728
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule name</td>
<td>The name of the policy rule, configured through the <code>policy rule</code> command.</td>
</tr>
<tr>
<td>Condition name</td>
<td>The name of the condition configured for this rule.</td>
</tr>
<tr>
<td>Action name</td>
<td>The name of the action configured for this rule.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Packets</th>
<th>The number of packets that match this rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes</td>
<td>The number of bytes that match this rule.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

policy rule

Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

MIB Objects

alaQoSRuleTable
  - alaQoSRuleName
  - alaQoSRuleEnabled
  - alaQoSRuleSource
  - alaQoSRulePrecedence
  - alaQoSRuleActive
  - alaQoSRuleReflexive
  - alaQosRuleLog
  - alaQosRuleTrapEvents
  - alaQosRuleSave
  - alaQoSRuleCondition
  - alaQoSRuleAction
show policy rule

Displays information about pending and applied policy rules.

show [applied] policy rule [rule_name]

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applied</td>
<td>Displays only policy rules that have been applied.</td>
</tr>
<tr>
<td>rule_name</td>
<td>The name of the rule for which you want to display information; or a wild-</td>
</tr>
<tr>
<td></td>
<td>card sequence of characters for displaying information about rules with</td>
</tr>
<tr>
<td></td>
<td>similar names. Use an asterisk (*) to indicate a wildcard character.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C6/T48C6/</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Information for all rules is displayed unless rule_name is specified.
- Use the show active policy rule command to display only active rules that are currently being enforced on the switch.

Examples

-> show policy rule
Rule name : r1
  Condition name = c1,
  Action name   = a1
Rule name : r2
  State        = new,
  Condition name = c2,
  Action name   = a1
Rule name : r3
  State        = new,
  Condition name = c2,
  Action name   = a2

-> show applied policy rule
Rule name : r1
  Condition name = c1,
  Action name   = a1
**output definitions**

<table>
<thead>
<tr>
<th>Rule name</th>
<th>The name of the policy rule, configured through the <strong>policy rule</strong> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>This field appears if the rule was created or modified but not yet applied to the QoS configuration. When the <strong>qos apply</strong> command is issued, this field no longer displays.</td>
</tr>
<tr>
<td>Condition name</td>
<td>The name of the condition configured for this rule.</td>
</tr>
<tr>
<td>Action name</td>
<td>The name of the action configured for this rule.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**policy rule**

Configures a policy rule on the switch. A rule is made up of a condition (for classifying incoming traffic) and an action (to be applied to outgoing traffic).

**MIB Objects**

- alaQoSRuleTable
  - alaQoSRuleName
  - alaQoSRuleEnabled
  - alaQoSRuleSource
  - alaQoSRulePrecedence
  - alaQoSRuleActive
  - alaQoSRuleReflexive
  - alaQoSRuleLog
  - alaQoSRuleTrapEvents
  - alaQoSRuleSave
  - alaQoSRuleCondition
  - alaQoSRuleAction
show policy validity period

Displays information about policy validity periods.

show policy validity period [name]

Syntax Definitions

name The name of the validity period.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- Information for all validity periods is displayed unless name is specified.
- Use the show policy rule command to display the validity period that is associated with a policy rule.

Examples

-> show policy validity-period
Validity period name = tuesday
  State             = new,
  Days              = tuesday

Validity period name = february
  Months            = february

-> show applied policy validity-period
Validity period name = february
  Months            = february

output definitions

Validity period name The name of the policy validity period, configured through the iec message-type priority command.

State This field appears if the validity period was created or modified but not yet applied to the QoS configuration. When the qos apply command is issued, this field no longer displays.
**output definitions**

<table>
<thead>
<tr>
<th>Days</th>
<th>The days of the week the validity period is active, configured through the <code>iec message-type priority</code> command. If this field does not appear, then the validity period is not restricted to specific days.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Months</td>
<td>The months during which the validity period is active, configured through the <code>iec message-type priority</code> command. If this field does not appear, then the validity period is not restricted to specific months.</td>
</tr>
<tr>
<td>Hours</td>
<td>The time of day the validity period begins and ends, configured through the <code>iec message-type priority</code> command. If this field does not appear, then the validity period is not restricted to a specific time.</td>
</tr>
<tr>
<td>Interval</td>
<td>The date and time a validity period interval begins and ends, configured through the <code>iec message-type priority</code> command. If this field does not appear, then the validity period is not restricted to a specific date and time interval.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `iec message-type priority` Configures a validity period that specifies days, times, and/or months during which an associated policy rule is in effect.

**MIB Objects**

`alaQoSValidityPeriodTable`
- `alaQoSValidityPeriodName`
- `alaQoSValidityPeriodSource`
- `alaQoSValidityPeriodDays`
- `alaQoSValidityPeriodDaysStatus`
- `alaQoSValidityPeriodMonths`
- `alaQoSValidityPeriodMonthsStatus`
- `alaQoSValidityPeriodHour`
- `alaQoSValidityPeriodHourStatus`
- `alaQoSValidityPeriodEndHour`
- `alaQoSValidityPeriodInterval`
- `alaQoSValidityPeriodIntervalStatus`
- `alaQoSValidityPeriodEndInterval`

`alaQoSAppliedValidityPeriodTable`
- `alaQoSAppliedValidityPeriodName`
- `alaQoSAppliedValidityPeriodSource`
- `alaQoSAppliedValidityPeriodDays`
- `alaQoSAppliedValidityPeriodDaysStatus`
- `alaQoSAppliedValidityPeriodMonths`
- `alaQoSAppliedValidityPeriodMonthsStatus`
- `alaQoSAppliedValidityPeriodHour`
- `alaQoSAppliedValidityPeriodHourStatus`
- `alaQoSAppliedValidityPeriodEndHour`
- `alaQoSAppliedValidityPeriodInterval`
- `alaQoSAppliedValidityPeriodIntervalStatus`
- `alaQoSAppliedValidityPeriodEndInterval`
**show active policy list**

Displays information about applied policy lists that are active (enabled) on the switch.

```bash
show active policy list [list_name]
```

**Syntax Definitions**

`list_name` The name of the list for which you want to display information; or a wildcard sequence of characters for displaying information about lists with similar names. Use an asterisk (*) to indicate a wildcard character.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Information for all active rules is displayed unless a `list_name` is specified.
- Use the `show policy list` command to display inactive as well as active policy lists.
- Applied lists may or may not be active on the switch. Applied lists are inactive if they have been administratively disabled with the `disable` option in the `policy list` command.
- The display may include any of the following characters:

<table>
<thead>
<tr>
<th>character</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Indicates that the policy list has been modified or has been created since the last <code>qos apply</code>.</td>
</tr>
<tr>
<td>-</td>
<td>Indicates the policy list is pending deletion.</td>
</tr>
<tr>
<td>#</td>
<td>Indicates that the policy list differs between the pending/applied lists.</td>
</tr>
</tbody>
</table>
Examples

```plaintext
-> show active policy list
```

<table>
<thead>
<tr>
<th>Group Name</th>
<th>From</th>
<th>Type</th>
<th>Enabled</th>
<th>Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>list1</td>
<td>cli</td>
<td>unp</td>
<td>Yes</td>
<td>r1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>r2</td>
</tr>
<tr>
<td>+list2</td>
<td>cli</td>
<td>unp</td>
<td>Yes</td>
<td>r3</td>
</tr>
<tr>
<td>egress_list1</td>
<td>cli</td>
<td>egress</td>
<td>Yes</td>
<td>r1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>r2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>r3</td>
</tr>
</tbody>
</table>

output definitions

- **Group Name**: The name of the policy list. Configured through the `policy list` command. A plus sign (+) preceding a policy list name indicates that the list was modified or created since the last `qos apply`.
- **From**: Where the list originated.
- **Type**: The type of rule (`unp, egress, apf`). Configured through the `policy list` command. Note that the default policy list is not shown. Use the `show policy rule` command to display rules that are members of the default policy list.
- **Enabled**: Whether or not the rule is enabled. Configured through the `policy list` command.
- **Entries**: The QoS policy rules that are grouped together in this policy list. Configured through the `policy list` command.

Release History

Release 7.2.1; command was introduced.

Related Commands

- `show policy list`: Displays information about pending and applied policy lists.
- `show policy rule`: Displays information about pending and applied policy rules

MIB Objects

```
alaQoSRuleGroupsTable
  alaQoSRuleDefaultList
  alaQoSRuleGroupsName
  alaQoSRuleGroupsSource
  alaQoSRuleGroupsType
  alaQoSRuleGroupsEnabled
  alaQoSRuleGroupsStatus
alaQosAppliedRuleGroupsTable
  alaQosAppliedRuleGroupsName
  alaQosAppliedRuleGroupsSource
  alaQosAppliedGroupsType
  alaQosAppliedGroupsEnabled
  alaQosAppliedRuleGroupsStatus
```
show policy list

Displays information about pending and applied policy lists.

show [applied] policy list [list_name]

Syntax Definitions

applied Displays only those policy lists that have been applied to the switch configuration.

list_name The name of the list to display information; or a wildcard sequence of characters for displaying information about lists with similar names. Use an asterisk (*) to indicate a wildcard character.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Information for all rules is displayed unless a list_name is specified.
- Use the show active policy list command to display only active policy lists that are currently enforced on the switch.
- The display may include any of the following characters:

<table>
<thead>
<tr>
<th>character</th>
<th>definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Indicates that the policy list has been modified or has been created since the last qos apply.</td>
</tr>
<tr>
<td>-</td>
<td>Indicates the policy list is pending deletion.</td>
</tr>
<tr>
<td>#</td>
<td>Indicates that the policy list differs between the pending/applied lists.</td>
</tr>
</tbody>
</table>

Examples

-> show policy list

<table>
<thead>
<tr>
<th>Group Name</th>
<th>From</th>
<th>Type</th>
<th>Enabled</th>
<th>Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>list1</td>
<td>cli</td>
<td>unp</td>
<td>Yes</td>
<td>rl</td>
</tr>
</tbody>
</table>
QoS Policy Commands

+list2                cli  unp  Yes  r2
r2

-> show applied policy list
Group Name               From  Type    Enabled  Entries
--------------------------------+-----+-------+--------+--------------------------
list1                      cli  unp  Yes   r1
r2

output definitions

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Group Name | The name of the policy list. Configured through the `policy list` command. A plus sign (+) preceding a policy list name indicates that the list was modified or created since the last `qos apply`.
| From       | Where the list originated. |
| Type       | The type of rule (unp, egress, appfp). Configured through the `policy list` command. Note that the default policy list is not shown. Use the `show policy rule` command to display rules that are members of the default policy list. |
| Enabled    | Whether or not the rule is enabled. Configured through the `policy list` command. |
| Entries    | The QoS policy rules that are grouped together in this policy list. Configured through the `policy list` command. |

Release History

Release 7.2.1; command was introduced.

Related Commands

show active policy list
Displays only those policy lists that are currently being enforced on the switch.

show policy rule
Displays information about pending and applied policy rules

MIB Objects

alaQoSRuleGroupsTable
alaQoSRuleDefaultList
alaQoSRuleGroupsName
alaQoSRuleGroupsSource
alaQoSRuleGroupsType
alaQoSRuleGroupsEnabled
alaQoSRuleGroupsStatus
alaQosAppliedRuleGroupsTable
alaQosAppliedRuleGroupsName
alaQosAppliedRuleGroupsSource
alaQosAppliedGroupsType
alaQosAppliedGroupsEnabled
alaQosAppliedGroupsStatus
show policy ipv4-summary

Displays all the IPv4 networks that are currently matched by ACLs on the system.

show policy ipv4-summary [rule rule_name]

Syntax Definitions

rule_name

The name of the policy rule.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specifying the rule name displays the detailed summary for the corresponding rule. If no rule name is specified, then the summary for each rule is displayed in a tabular form.

- If there is an explicit default rule that is set to deny, the same is displayed in the output.

Examples

`-> show policy ipv4-summary`
Legends:
P= Protocol
Act= Action (d = deny, a = accept)

<table>
<thead>
<tr>
<th>Rule</th>
<th>P</th>
<th>Source IP/ Source Group</th>
<th>Destination IP/ Destination Group</th>
<th>VRF Name</th>
<th>Act</th>
<th>Hit Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>rle-rule3</td>
<td>IP</td>
<td>224.0.0.0/4</td>
<td>224.0.0.0/4</td>
<td>default</td>
<td>a</td>
<td>30129</td>
</tr>
<tr>
<td>rle-rule4</td>
<td>UDP</td>
<td>0.0.0.0/0</td>
<td>0.0.0.0/0</td>
<td>default</td>
<td>d</td>
<td>1020202</td>
</tr>
<tr>
<td>rle-rule1</td>
<td>IP</td>
<td>192.168.10.0/*</td>
<td>192.168.20.0/24</td>
<td>guest</td>
<td>a</td>
<td>458723011</td>
</tr>
<tr>
<td>rle-rule2</td>
<td>IP</td>
<td>192.168.30.0/24</td>
<td>192.168.10.0/24</td>
<td>enterprise</td>
<td>a</td>
<td>458723011</td>
</tr>
</tbody>
</table>

`-> show policy ipv4-summary rule rle-rule2`

output definitions

<table>
<thead>
<tr>
<th>Rule</th>
<th>Name of the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>The associated IP protocol.</td>
</tr>
<tr>
<td>Source IP/ Source Group</td>
<td>The IPv4 address of the source or source group.</td>
</tr>
<tr>
<td>Destination IP/Destination Group</td>
<td>The IPv4 address of the destination or destination group.</td>
</tr>
<tr>
<td>VRF Name</td>
<td>The name of the VRF.</td>
</tr>
<tr>
<td>Act</td>
<td>The name of the action.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>The sum of packet counts from all NIs matching the corresponding rule.</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1.R02; command introduced.

Related Commands

show active policy list Displays only those policy lists that are currently being enforced on the switch.

show policy rule Displays information about pending and applied policy rules

MIB Objects

N/A
**show policy ipv6-summary**

Displays all the IPv6 networks that are currently matched by ACLs on the system.

`show policy ipv6-summary [rule rule_name]`

### Syntax Definitions

`rule_name`  
The name of the policy rule.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4/E/V48C8</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Specifying the rule name displays the detailed summary for the corresponding rule. If no rule name is specified, then the summary for each rule is displayed in a tabular form.

- If there is an explicit default rule that is set to deny, the same is displayed in the output.

### Examples

```
-> show policy ipv6-summary
Legends:
P= Protocol
Act= Action (d = deny, a = accept)

<table>
<thead>
<tr>
<th>Rule</th>
<th>P</th>
<th>Source IP/ Source Group</th>
<th>VRF Name</th>
<th>Act</th>
<th>Hit Count</th>
<th>Destination IP/ Destination Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>rle-Rule1</td>
<td>IP</td>
<td>2001:abcd:1100:200::/64</td>
<td>default</td>
<td>a</td>
<td>02020</td>
<td>2020:acdc:1010:100::/64</td>
</tr>
</tbody>
</table>

-> show policy ipv6-summary rule rle-Rule2

Rule name   : rle-Rule2,
Protocol     : IP,
Source IP    : 2001:abcd:1100:200::/64,
Destination IP: 2020:acdc:1010:100::/64,
VRF Name     : default,
```
**Hit Count** : 458723011

### output definitions

<table>
<thead>
<tr>
<th><strong>Rule</strong></th>
<th>Name of the rule.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>P</strong></td>
<td>The associated IP protocol.</td>
</tr>
<tr>
<td><strong>Source IP/ Source Group</strong></td>
<td>The IPv6 address of the source or source group.</td>
</tr>
<tr>
<td><strong>Destination IP/Destination Group</strong></td>
<td>The IPv6 address of the destination or destination group.</td>
</tr>
<tr>
<td><strong>VRF Name</strong></td>
<td>The name of the VRF.</td>
</tr>
<tr>
<td><strong>Act</strong></td>
<td>The name of the action.</td>
</tr>
<tr>
<td><strong>Hit Count</strong></td>
<td>The sum of packet counts from all NIs matching the corresponding rule.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.3.1.R02; command introduced.
Release 8.4.1.R02; OmniSwitch 6860 and OmniSwitch 6865 support added.

### Related Commands

- **show active policy list**
  - Displays only those policy lists that are currently being enforced on the switch.
- **show policy rule**
  - Displays information about pending and applied policy rules

### MIB Objects

N/A
This chapter describes CLI commands used for managing policies downloaded to the switch from an attached LDAP server. Policy rules can be created on an attached server through the PolicyView GUI application. Policy rules can also be created on the switch directly through CLI or SNMP commands. This chapter describes commands related to managing LDAP policies only. See Chapter 36, “QoS Commands,” for information about commands for creating and managing policies directly on the switch.

The policy commands are based on RFC 2251 and RFC 3060.

MIB information for policy server commands is as follows:

   Filename: ALCATEL-IND1-POLICY-MIB.mib  
   Module: alcatelIND1PolicyMIB

The policy server commands are summarized here:

  policy server load
  policy server flush
  policy server
  show policy server
  show policy server long
  show policy server statistics
  show policy server rules
  show policy server events
**policy server load**

Downloads policies from an LDAP server. These policies are created through the PolicyView management application.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Policies are downloaded to the switch from the directory server with the highest preference setting; this server must be enabled and operational (able to bind).

**Examples**

```
-> policy server load
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **policy server flush**
  Removes all cached LDAP policy data from the switch.

**MIB Objects**

- serverPolicyDecision
policy server flush

Removes all cached LDAP policy data from the switch.

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use this command to remove LDAP policies. Policies configured through the CLI or SNMP are not removed.

Examples

-> policy server flush

Release History
Release 7.1.1; command introduced.

Related Commands

policy server load Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

MIB Objects

serverPolicyDecision
**policy server**

Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

```
policy server ip_address [port port_number] [admin-state {enable | disable}] [preference preference] [user user_name password password] [searchbase search_string] [ssl | no ssl]
```

```
no policy server ip_address [port port_number]
```

### Syntax Definitions

- **ip_address**: The IP address of the LDAP-enabled directory server.
- **port_number**: The TCP/IP port number used by the switch to connect to the directory server.
- **enable**: Enables the specified policy server to download rules to the switch. The policy servers are **up** by default.
- **disable**: Prevents the specified policy server from downloading rules to the switch.
- **preference**: Determines which directory server is used for policy downloads when multiple servers are configured. The range is 0–255. The server with the highest value is used as the policy server. If that server becomes unavailable, the server with the next highest preference value is used for policy downloads.
- **user_name**: The user name for accessing the database entries on the directory server. When spaces are used in the user name, quotation marks must be included: (e.g. “Directory Manager”).
- **password**: The password associated with the user name. The password must match the password defined on the directory server.
- **search_string**: The root of the directory required for searching the policy information. Typically, the search_string includes o=organization and c=country. For example, o=company and c=country.
- **ssl**: Enables a Secure Socket Layer between the switch and the policy server.
- **no ssl**: Disables a Secure Socket Layer between the switch and the policy server.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>up</td>
</tr>
<tr>
<td>port_number</td>
<td>389 (SSL disabled)</td>
</tr>
<tr>
<td></td>
<td>636 (SSL enabled)</td>
</tr>
<tr>
<td>preference</td>
<td>0</td>
</tr>
<tr>
<td>ssl</td>
<td>no ssl</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you change the port number, another entry is added to the policy server table; the existing port number is not changed. To remove a port number, use the no form of this command with the relevant policy server IP address and the port number you want to remove.

Examples

-> policy server 222.22.22.2 port 345 user dirmgr password secret88 searchbase ou=qos,o=company,c=country

Release History

Release 7.1.1; command introduced.

Related Commands

show policy server Displays information about policies downloaded from an LDAP server.

MIB Objects

DIRECTORYSERVERTABLE
  directoryServerAddress
directoryServerPort
directoryServerAdminStatus
directoryServerPreference
directoryServerUserId
directoryServerAuthenticationType
directoryServerPassword
directoryServerSearchbase
directoryServerEnableSSL
show policy server

Displays information about servers from which policies can be downloaded to the switch.

show policy server

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays basic information about policy servers. Use the `show policy server long` command to display more details about the servers.

Examples

-> show policy server

<table>
<thead>
<tr>
<th>Server</th>
<th>IP Address</th>
<th>port</th>
<th>enabled</th>
<th>status</th>
<th>primary</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>208.19.33.112</td>
<td>389</td>
<td>Yes</td>
<td>Up</td>
<td>X</td>
</tr>
<tr>
<td>2</td>
<td>208.19.33.66</td>
<td>400</td>
<td>No</td>
<td>Down</td>
<td>-</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Server</th>
<th>The index number corresponding to the LDAP server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the LDAP server.</td>
</tr>
<tr>
<td>port</td>
<td>The TCP/IP port number used by the switch to connect to the policy server.</td>
</tr>
<tr>
<td>enabled</td>
<td>Whether or not the policy server is enabled.</td>
</tr>
<tr>
<td>status</td>
<td>The state of the policy server, <strong>Unkn</strong>, <strong>Up</strong> or <strong>Down</strong>.</td>
</tr>
<tr>
<td>primary</td>
<td>Indicates whether the server is the primary server; this server can be used for the next download of policies; only one server is a primary server.</td>
</tr>
</tbody>
</table>


**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **policy server**

  Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

**MIB Objects**

- **directoryServerTable**
  - **directoryServerAddress**
  - **directoryServerPort**
  - **directoryServerAdminState**
**show policy server long**

Displays more detailed information about an LDAP policy server.

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays detailed information about policy servers. Use the `show policy server` command to display basic information about policy servers.

### Examples

```
-> show policy server long
LDAP server 0
  IP address : 155.132.44.98,
  TCP port : 16652,
  Enabled : Yes,
  Operational status : Unkn,
  Preference : 99,
  Authentication : password,
  SSL : Disabled,
  login DN : cn=Directory Manager,
  searchbase : ou:4.1, cn=policyRoot, o=company.fr
  Last load time : 09/13/01 16:38:18
LDAP server 1
  IP address : 155.132.48.27,
  TCP port : 21890,
  Enabled : Yes,
  Operational status : Unkn,
  Preference : 50,
  Authentication : password,
  SSL : Disabled,
  login DN : cn=Directory Manager,
  searchbase : o=company.fr
  Last load time : 00/00/00 00:00:00
```
### Policy Server Commands

**show policy server long**

#### Release History

Release 7.1.1; command introduced.

#### Related Commands

- **policy server**: Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

#### MIB Objects

- `directoryServerTable`  
  - `directoryServerAddress`  
  - `directoryServerPort`  
  - `directoryServerPreference`  
  - `directoryServerAuthenticationType`  
  - `directoryServerSearchbase`  
  - `directoryServerUserId`  
  - `directoryServerPassword`  
  - `directoryServerCacheChange`  
  - `directoryServerLastChange`  
  - `directoryServerAdminStatus`  
  - `directoryServerOperStatus`
show policy server statistics

Displays statistics about policy directory servers.

show policy server statistics

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays statistics about server downloads. For information about server parameters, use the `show policy server` command.

**Examples**

```
-> show policy server statistics
Server          IP Address      port accesses delta successes delta errors delta
------------------------------+-----------------+-----------+---------+-----------+----------------+-----------+--------+--------+
  1      155.132.44.98    16652        793   793      295   295        0     0
  2      155.132.48.27    21890        0     0        0     0        0     0
```

**output definitions**

- **Server**: The index number corresponding to the server.
- **IP Address**: The IP address of the LDAP server.
- **port**: The TCP/IP port number used by the switch to connect to the policy server.
- **accesses**: The number of times the server was polled by the switch to download policies.
- **delta**: The change in the number of accesses since the last time the policy server was accessed.
- **successes**: The number of times the server was polled by the switch to download policies and the policies were successfully downloaded.
**output definitions**

| delta          | The change in the number of successful policy downloads since the last time the policy server was accessed. |
| errors         | The number of errors returned by the server. |
| delta          | The change in the number of errors returned by the server since the last time the policy server was accessed. |

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**policy server**

Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

**MIB Objects**

`policyStatsTable`
- `policyStatsAddress`
- `policyStatsServerPort`
- `policyStatsAccessCount`
- `policyStatsSuccessAccessCount`
- `policyStatsNotFoundCount`
**show policy server rules**

Displays the names of policies originating from a directory server, that have been downloaded to the switch.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays information about policies created on directory servers only. Chapter 36, “QoS Commands,” for information about configuring and displaying policies directly on the switch.

**Examples**

```plaintext
-> show policy server rules
Num  name     prio scope  status
----  --------  ----  ------  ------
1     QoSRule1  0     Provisioned Active
2     QoSrule2  0     Provisioned Active
```

**output definitions**

- **Num**: An index number corresponding to the policy rule.
- **name**: The name of the policy rule; only rules configured through PolicyView are displayed in this table.
- **prio**: The priority or preference of the rule. Indicates the order in which rules can be checked to match to the incoming traffic. If two or more rules apply to the traffic, the rule with the highest preference is applied. Preference is determined when the rule is created.
- **scope**: The type of rule. ** Provisioned** is the only type valid for the current release.
output definitions (continued)

| status          | The status of the rule: **Active** indicates that the rule is available in the QoS software on the switch and is available to be applied to the traffic; **notInService** means the rule can be pushed to the QoS software in the future but is not available yet (typically because of a variable validity period); **notReady** indicates that the rule can never be pushed to the QoS software because its validity period has expired or because it has been disabled through SNMP. |

---

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**policy server load**

Downloads policies from a LDAP server. These policies are created through the PolicyView management application.

**MIB Objects**

policyRuleNamesTable
  - policyRuleNamesIndex
  - policyRuleNamesName
  - policyRuleOperStatus
show policy server events

Displays any events related to a directory server on which policies are stored.

show policy server events

Syntax Definitions

N/A

Defaults

The display is limited to 50 events.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

The Policy Manager initialization event is always the first event logged.

Examples

```
-> show policy server events
Event Time          event description
-------------------+----------------------------------------------------------
09/13/01 16:38:15  Policy manager log init
09/13/01 16:38:17  LDAP server 155.132.44.98/16652 defined
09/13/01 16:38:17  LDAP server 155.132.44.98/21890 defined
09/13/01 16:38:18  PDP optimization: PVP day-of-week all 1
09/13/01 16:38:18  PDP optimization: PVP Month all 1
09/13/01 16:38:18  PDP optimization: PVP Month all 1
09/13/01 16:38:18  PDP optimization: PVP Month all 1
09/13/01 16:38:18  IP address and mask make bad address change on destination IP address 155.132.44.98:155.132.44.101
```

output definitions

<table>
<thead>
<tr>
<th>Event Time</th>
<th>The date and time the policy event occurred.</th>
</tr>
</thead>
<tbody>
<tr>
<td>event description</td>
<td>A description of the event.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Related Commands

policy server

Configures operational parameters for an LDAP-enabled directory server on which policies are stored.

MIB Objects

policyEventTable
  policyEventCode
  policyEventDetailString
  policyEventIndex
  policyEventTime
This chapter includes descriptions for authentication, authorization, and accounting (AAA) commands. The commands are used for configuring the type of authentication as well as the AAA servers and the local user database on the switch.

- Authenticated Switch Access. Authenticates users into the switch to manage the switch. User information is stored on a RADIUS, TACACS+, LDAP or information may be stored locally in the switch user database.

- Local user database. User information may be configured for Authenticated Switch Access. For functional management access, users may be allowed to access specific command families or domains.

MIB information for the AAA commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALCATEL-IND1-AAA-MIB.mib</td>
<td>alcatelIND1AAAMIB</td>
</tr>
<tr>
<td>ALCATEL-IND1-SYSTEM-MIB.mib</td>
<td>alcatelIND1SystemMIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>Authentication servers</th>
<th>AAA Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa radius-server</td>
</tr>
<tr>
<td></td>
<td>aaa radius-server health-check</td>
</tr>
<tr>
<td></td>
<td>aaa radius unp-profile-precedence</td>
</tr>
<tr>
<td></td>
<td>aaa test-radius-server</td>
</tr>
<tr>
<td></td>
<td>aaa tacacs+-server</td>
</tr>
<tr>
<td></td>
<td>aaa tacacs command-authorization</td>
</tr>
<tr>
<td></td>
<td>aaa ldap-server</td>
</tr>
<tr>
<td></td>
<td>show aaa server</td>
</tr>
<tr>
<td></td>
<td>show aaa server statistics</td>
</tr>
<tr>
<td></td>
<td>aaa radius-server clear-statistics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Federal Information Processing Standards (FIPS)</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>system fips admin-state</td>
<td></td>
</tr>
<tr>
<td>show system fips</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authenticated Switch Access</th>
<th>Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authentication</td>
<td></td>
</tr>
<tr>
<td>aaa console admin-only</td>
<td></td>
</tr>
<tr>
<td>aaa authentication default</td>
<td></td>
</tr>
<tr>
<td>aaa accounting session</td>
<td></td>
</tr>
<tr>
<td>aaa accounting command</td>
<td></td>
</tr>
<tr>
<td>show aaa authentication</td>
<td></td>
</tr>
<tr>
<td>show aaa accounting</td>
<td></td>
</tr>
</tbody>
</table>
### AAA Commands

<table>
<thead>
<tr>
<th>Port-based Network Access Control (Access Guardian)</th>
<th>aaa device-authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>aaa accounting</td>
</tr>
<tr>
<td></td>
<td>aaa accounting radius calling-station-id</td>
</tr>
<tr>
<td></td>
<td>aaa 802.1x re-authentication</td>
</tr>
<tr>
<td></td>
<td>aaa interim-interval</td>
</tr>
<tr>
<td></td>
<td>aaa session-timeout</td>
</tr>
<tr>
<td></td>
<td>aaa session console</td>
</tr>
<tr>
<td></td>
<td>aaa inactivity-logout</td>
</tr>
<tr>
<td></td>
<td>aaa radius nas-port-id</td>
</tr>
<tr>
<td></td>
<td>aaa radius nas-identifier</td>
</tr>
<tr>
<td></td>
<td>aaa radius nas-ip-address</td>
</tr>
<tr>
<td></td>
<td>aaa radius mac-format</td>
</tr>
<tr>
<td></td>
<td>aaa profile</td>
</tr>
<tr>
<td></td>
<td>show aaa device-authentication</td>
</tr>
<tr>
<td></td>
<td>show aaa accounting</td>
</tr>
<tr>
<td></td>
<td>show aaa config</td>
</tr>
<tr>
<td></td>
<td>show aaa radius config</td>
</tr>
<tr>
<td></td>
<td>show aaa radius health-check-config</td>
</tr>
<tr>
<td></td>
<td>show aaa profile</td>
</tr>
<tr>
<td></td>
<td>show aaa session console config</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local User Database and Partitioned Management</th>
<th>user</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>password</td>
</tr>
<tr>
<td></td>
<td>super-password</td>
</tr>
<tr>
<td></td>
<td>user password-size min</td>
</tr>
<tr>
<td></td>
<td>user password-expiration</td>
</tr>
<tr>
<td></td>
<td>user allow-ssh</td>
</tr>
<tr>
<td></td>
<td>show user</td>
</tr>
<tr>
<td></td>
<td>show aaa priv hexa</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Password Policy</th>
<th>super-password</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>user password-expiration</td>
</tr>
<tr>
<td></td>
<td>user password-policy cannot-contain-username</td>
</tr>
<tr>
<td></td>
<td>user password-policy cannot-contain-consecutive-characters</td>
</tr>
<tr>
<td></td>
<td>user password-policy min-uppercase</td>
</tr>
<tr>
<td></td>
<td>user password-policy min-lowercase</td>
</tr>
<tr>
<td></td>
<td>user password-policy min-digit</td>
</tr>
<tr>
<td></td>
<td>user password-policy min-nonalpha</td>
</tr>
<tr>
<td></td>
<td>user password-history</td>
</tr>
<tr>
<td></td>
<td>super-password</td>
</tr>
<tr>
<td></td>
<td>user password-min-age</td>
</tr>
<tr>
<td></td>
<td>user password-expiration</td>
</tr>
<tr>
<td></td>
<td>show user</td>
</tr>
<tr>
<td></td>
<td>show user password-policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Lockout Settings</th>
<th>user lockout-window</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>user lockout-threshold</td>
</tr>
<tr>
<td></td>
<td>user lockout-duration</td>
</tr>
<tr>
<td></td>
<td>user lockout unlock</td>
</tr>
<tr>
<td></td>
<td>show user</td>
</tr>
<tr>
<td></td>
<td>show user lockout-setting</td>
</tr>
<tr>
<td>AAA Commands</td>
<td>Command</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Authenticated Switch Access - Enhanced Mode | aaa switch-access mode  
                      aaa switch-access ip-lockout-threshold  
                      aaa switch-access banned-ip release  
                      aaa switch-access priv-mask  
                      aaa switch-access management-stations admin-state  
                      aaa switch-access management-stations  
                      show aaa switch-access mode  
                      show aaa switch-access ip-lockout-threshold  
                      show aaa switch-access banned-ip  
                      show aaa switch-access priv-mask  
                      show aaa switch-access management-stations  
                      show aaa switch-access hardware-self-test  
                      show aaa switch-access process-self-test |
| Common Criteria     | aaa common-criteria admin-state  
                      show aaa common-criteria config  
                      aaa certificate update-ca-certificate  
                      aaa certificate update-crl  
                      aaa certificate generate-rsa-key key-file  
                      aaa certificate generate-self-signed  
                      aaa certificate view  
                      aaa certificate verify ca-certificate  
                      aaa certificate delete  
                      aaa certificate generate-csr |
| Public Key Infrastructure (PKI)       | ssl pki client validate-certificate admin-state  
                      ssl pki client mutual-authentication admin-state  
                      ssl pki server mutual-authentication admin-state  
                      ssl pki tls version  
                      show ssl pki config |
| Cipher Security Level | ssl cipher  
                      show ssl ciphers all  
                      show ssl ciphers config |
| Kerberos Snooping   | kerberos inactivity-timer  
                      kerberos ip-address  
                      kerberos server-timeout  
                      kerberos authentication-pass policy-list-name  
                      kerberos authentication-pass domain  
                      clear kerberos statistics  
                      show kerberos configuration  
                      show kerberos users  
                      show kerberos statistics |
| Joint Interoperability Test Command (JITC) | aaa jitc admin-state  
                      show aaa jitc config |
aaa radius-server

Configures a RADIUS server for Authenticated Switch Access and device authentication.

    aaa radius-server server_name host [hostname | ip_address | ipv6_address] [hostname2 | ip_address2 | ipv6_address2] {key secret | hash-key hash_secret | prompt-key}[salt salt | hash-salt hash_salt] [retransmit retries] [timeout seconds] [auth-port auth_port] [acct-port acct_port] [vrf-name name] [ssl | no ssl]

no aaa radius-server server_name

Syntax Definitions

server_name  The name of the RADIUS server.
hostname     The host name (DNS name) of the primary RADIUS server. The host name or IP address is required when creating a server.
ip_address | ipv6_address The IPv4 or IPv6 address of the primary RADIUS server. An IP address or host name is required when creating a server.
hostname2   The host name (DNS name) of an optional backup RADIUS server.
ip_address2 | ipv6_address2 The IPv4 or IPv6 address of an optional backup RADIUS server.
secret      The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. Required when creating a server.

hash_secret A shared secret that the switch saves with a hashing algorithm.
prompt-key   This option enters the secret key in a obscured format rather than as clear text. When this option is selected, press the Enter key. A prompt appears asking for the secret key. Re-enter the key and only if both entries match, the command is accepted. The key provided in this mode is not displayed on the CLI as text.
salt         The input given through ‘salt’ will be used to add randomness to the encryption of the key. The maximum length of the salt is 15 characters and must be in clear text format. By default, system time will be taken as default salt value.

hash-salt   The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt should not exceed 64 characters.
retries     The number of retries the switch makes to authenticate a user before trying the backup server (hostname2 or ip_address2).
seconds     The timeout for server replies to authentication requests.
auth_port   The UDP destination port for authentication requests.
acct_port   The UDP destination port for accounting requests.
name        The name of the VRF to be used to access the server.
ssl         Enables Transport Layer Security (TLS) between the switch and the RADIUS server.
no ssl      Disables Transport Layer Security (TLS) between the switch and the RADIUS server.
AAA Commands

aaa radius-server

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>retries</td>
<td>3</td>
</tr>
<tr>
<td>seconds</td>
<td>2</td>
</tr>
<tr>
<td>auth_port</td>
<td>1812</td>
</tr>
<tr>
<td>acct_port</td>
<td>1813</td>
</tr>
<tr>
<td>ssl</td>
<td>no ssl</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- A host name (or IP address) and a secret are required when configuring a server.
- The server and the backup server must both be RADIUS servers.
- Use the no form of the command to remove a RADIUS server from the configuration. Only one server can be deleted at a time.
- A host name (or IP address) and a secret key are required when configuring a server.
- If key and hash-key parameters are both configured, the hash-key value is given priority over key.
- The user configured or default salt along with the server name will be combined with 'key' and encrypted as a whole, the output of which will be displayed under ‘hash-key’.
- If salt and hash-salt parameters are both configured, the hash-salt value is given priority over salt.
- The special character ‘!’ and pure integers will not be accepted as a valid input for both the salt and hash-salt parameters.
- To use special characters in the salt value, enter the special character between "" double quotes.
- The input given through salt and hash-salt is encrypted and will be displayed as “hash-salt” in show configuration snapshot command.
- Backward compatibility for salt and hash-salt is not supported. In case of an accidental downgrade, a boot.cfg error is generated for that particular configuration, and re-configuration is required.
- RADIUS server can be configured on any VRF instance or the default VRF instance. However, all the RADIUS servers must reside on the same VRF instance.
- Enabling the RADIUS server health check feature is recommended for each RADIUS server to help improve the user authentication time. Use the aaa radius-server health-check command to enable this
AAA Commands

feature and the show aaa server command to determine the reachability status of each RADIUS server on which health check is enabled.

Examples

```
-> aaa radius-server pubs2 host 10.10.2.1 key wwwtoe timeout 5
-> no aaa radius-server pubs2

-> aaa radius-server radsrv1 host rad1_ipaddr key rad1_secret vrf-name rad_vrf
-> aaa radius-server “Rad1” host 10.10.10.2 key myorg salt mysalt
c7f5eee2c0f9b33e72e3482673fb6059

-> aaa radius-server rad1 prompt-key host 10.10.2.1
Enter Key: *******
Confirm Key: *******
```

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; prompt-key parameter added.
Release 8.4.1; IPv6 and SSL support for radius server added.
Release 8.6R1; salt and hash-salt parameters added.

Related Commands

- **show aaa server**: Displays information about AAA servers.
- **aaa authentication**: Specifies the AAA servers to be used for Authenticated Switch Access.
- **aaa device-authentication**: Specifies the AAA servers to use for Access Guardian device authentication.
- **aaa accounting session**: Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

- **aaaServerTable**
  - **aaasProtocol**
  - **aaasHostName**
  - **aaasIpAddress**
  - **aaasIpv6Address**
  - **aaasHostName2**
  - **aaasIpAddress2**
  - **aaasIpv6Address2**
  - **aaasRadKey**
  - **aaasRetries**
  - **aaasTimeout**
  - **aaasRadAuthPort**
  - **aaasRadAcctPort**
  - **aaasVrfName**
  - **aaasRadEnableSsl**
  - **aaasRadSalt**
  - **aaasRadSaltHash**
aaa radius-server health-check

Enables or disables the RADIUS server health check configuration for the specified RADIUS server. When this feature is enabled, individual RADIUS servers are polled at the specified time interval to determine whether the server is up or down.

```
aaa radius-server server_name health-check [poling-interval seconds | username user_name | password password | hash-key hash_secret | failover]
no aaa radius-server server_name health-check [failover]
```

**Syntax Definitions**

- `server_name`: The name of the RADIUS server for which a health check session is configured.
- `seconds`: The number of seconds after which a health check request is sent to the specified RADIUS server. The valid range is 60–600 seconds.
- `user_name`: The user name (up to 32 characters) to use in polling requests to the server.
- `password`: The password (up to 64 characters) to use in polling requests to the server.
- `hash_secret`: A shared secret that the switch saves with a hashing algorithm.
- `failover`: Triggers an attempt to re-authenticate users assigned to the authentication server down profile when the RADIUS server comes back up before the authentication server down timeout expires.

**Defaults**

By default, RADIUS server health check is disabled. When health check is enabled without specifying any of the optional parameters, the following default health check parameter values are set for the specified RADIUS server:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
<tr>
<td>user_name</td>
<td>alcatel</td>
</tr>
<tr>
<td>password</td>
<td>alcatel</td>
</tr>
<tr>
<td>failover</td>
<td>disabled</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Make sure the specified RADIUS server is defined on the switch before attempting to enable a health check session for that server. See the `aaa radius-server` command for more information on RADIUS server configuration.

- Each RADIUS server with health check enabled is polled at regular intervals (instead of checked sequentially) to determine if the server is up or down. Notification of the server status is then provided to help expedite the authentication process.

- User devices are typically assigned to a UNP authentication server down profile when the authentication server is down (unreachable).
  - If the `failover` option is disabled (the default) for the health check session, re-authentication is not attempted for the profile devices until the authentication server down timeout value expires.
  - If the `failover` option is enabled for the health check session, there is no waiting for the authentication server down timeout value to expire. When the health check session receives notification that a server has transitioned from down to up, a re-authentication attempt is immediately triggered for the profile devices.

- Use the `no` form of this command to disable health check.

- Use the `no` form of this command with the `failover` parameter to disable the failover operation.

Examples

```
-> aaa radius-server rad1 health-check
-> aaa radius-server rad1 health-check polling-interval 300
-> aaa radius-server rad1 health-check username admin password switch failover
-> no aaa radius-server rad1 health-check failover
-> no aaa radius-server rad1 health-check
```

Release History

Release 8.5R4; command introduced.

Related Commands

- `aaa radius-server` Configures or modifies a RADIUS server for Authenticated Switch Access and device authentication.
- `show aaa radius health-check` Displays the health check configuration for each RADIUS server.
- `show aaa server` Displays information about AAA servers configured for the switch.

MIB Objects

- `aaaServerTable` contains
  - `aaasHostName`
  - `aaasRadHealthCheck`
  - `aaasRadPollingInterval`
  - `aaasRadFailover`
  - `aaasRadUsername`
  - `aaasRadPassword`
aaa radius unp-profile-precedence

This command can be used to set the precedence to filter ID or tunnel private group ID attributes for selection of UNP profile in the event of both these attributes being returned from the RADIUS server.

`aaa radius unp-profile-precedence {tunnel-private-group-id | filter-id}`

**Syntax Definitions**

- **tunnel-private-group-id**: The tunnel private group ID attribute.
- **filter-id**: The filter ID RADIUS attribute.

**Defaults**

By default, filter ID will be given precedence over the tunnel private group ID.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `aaa radius unp-profile-precedence tunnel-private-group-id`
- `aaa radius unp-profile-precedence filter-id`

**Release History**

Release 8.5R4; command introduced.

**Related Commands**

- `aaa radius-server`: Configures or modifies a RADIUS server for Authenticated Switch Access and device authentication.
- `show aaa radius config`: Displays the global AAA attribute values and MAC address format.

**MIB Objects**

- `alaAaaRadUnpProfilePrecedence`
aaa test-radius-server

RADIUS test tool allows the user to test the RADIUS server reachability from the OmniSwitch. Use this command to start the authentication or accounting test for the specified user name and password.

`aaa test-radius-server server_name type {authentication user user_name password password [method {md5 | pap}] | accounting user user_name}`

**Syntax Definitions**

- `server_name`: RADIUS server name for which test has been configured.
- `authentication | accounting`: Type of test to run.
- `user_name`: User name configured on the server.
- `password`: Password for the given user name.
- `md5 | pap`: Authentication method for the test.

**Defaults**

By default, MD5 is used as the authentication method.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- RADIUS server must be configured on the switch to test the tool.
- The switch must have the following RADIUS server configuration before starting the test tool: RADIUS server name, acct-port, auth-port, secret key, retransmit count, and timeout. See the `aaa radius-server` command for more information on RADIUS server configuration.
- Supports multiple sessions (console, telnet, SSH) to test multiple RADIUS servers.
- The CLI of the user session (console, telnet, SSH) goes in the blocking state when the test is started. In the blocking state, no other command (CLI) is accepted. The blocking state of the CLI prompt of the switch can be terminated by pressing any key.
- Two IP addresses are configurable for a RADIUS server. When the test starts, the requests are sent to the first address. When all the requests to the first address time out, then the requests are sent to the second address.
**Examples**

-> aaa test-radius-server rad1 type authentication user admin password switch method MD5
-> aaa test-radius-server rad2 type authentication user admin password switch method pap
-> aaa test-radius-server rad1 type accounting user admin

**Release History**

Release 8.1.1; command introduced.

**Related Commands**

- **aaa authentication**
  Servers for authenticated switch access.

- **show aaa server**
  Displays information about AAA servers configured for the switch.

**MIB Objects**

N/A
aaa tacacs+-server

Configures or modifies a TACACS+ server for Authenticated Switch Access.

```
aaa tacacs+-server server_name host [hostname | ip_address | ipv6_address1] [hostname2 | ip_address2 | ipv6_address2] [key secret | prompt-key] [salt salt | hash-salt hash_salt] [timeout seconds] [port port] [vrf-name name]
```

no aaa tacacs+-server server

Syntax Definitions

- `server_name`: The name of the TACACS+ server.
- `hostname`: The host name (DNS name) of the primary TACACS+ server. The host name or IP address is required when creating a server.
- `ip_address`: The IP address of the primary TACACS+ server. An IP address or host name is required when creating a server.
- `ipv6_address1`: The IPv6 address of the primary TACACS+ server.
- `hostname2`: The host name (DNS name) of an optional backup TACACS+ server.
- `ip_address2`: The IP address of an optional backup TACACS+ server.
- `ipv6_address2`: The IPv6 address of an optional backup TACACS+ server.
- `secret`: The shared secret known to the switch and the server, but which is not sent over the network. Can be any text or hexadecimal string but MUST match the secret configured on the server. The secret is case-sensitive. Required when creating a server.
- `salt`: The input given through ‘salt’ will be used to add randomness to the encryption of the key. The maximum length of the salt is 15 characters, and must be in clear text format. By default, the system time will be taken as default salt value.
- `hash_salt`: The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt should not exceed 64 characters.
- `prompt-key`: This option enters the secret key in a obscured format rather than as clear text. When this option is selected, press the Enter key. A prompt appears asking for the secret key. Re-enter the key and only if both the entries match, the command is accepted. Password provided in this mode is not displayed on the CLI as text.
- `seconds`: The timeout for server replies to authentication requests.
- `port`: The port number for the primary TACACS+ server.
- `name`: The name of the VRF to be used to access the server.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>2</td>
</tr>
<tr>
<td>port</td>
<td>49</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of the command to remove a TACACS+ server from the configuration. Only one server may be deleted at a time.
- A host name (or IP address) and a secret are required when configuring a server.
- If key and hash-key parameters are both configured, the hash-key value is given priority over key.
- The user configured or default salt along with the server name will be combined with the key and encrypted as a whole, the output of which will be displayed under ‘hash-key’.
- If salt and hash-salt parameters are configured, the hash-salt value is given priority over salt.
- The special character ‘!’ and pure integers will not be accepted as a valid input for both salt and hashsalt.
- To use special characters in the salt value, enter them in between ”“ double quotes.
- The input given through salt and hash-salt is encrypted and will be displayed as ‘hash-salt’ in the show configuration snapshot command.
- Backward compatibility for salt and hash-salt is not supported. In case of an accidental downgrade, boot.cfg error is generated for that particular configuration, and re-configuration is required.
- The server and the backup server must both be TACACS+ servers.
- TACACS+ server can be configured on any VRF instance or the default VRF instance. However, all the TACACS+ servers must reside on the same VRF instance.

Examples

- > aaa tacacs+-server tpub host 10.10.2.2 key otna timeout 10
- > no aaa tacacs+-server tpub
- > aaa tacacs+-server T1 host 10.10.10.3 key myorg salt salt@123
- > aaa tacacs+-server tacsrv1 host tac1_ipaddr key tac1_secret vrf-name tac_vrf

- > aaa tacacs+-server tac1 prompt-key host 10.10.2.2
  Enter Key:  *******
  Confirm Key:  *******
- > aaa tacacs+-server T1 host 2001:400::f00::2 key testing123 timeout 2
- > aaa tacacs+-server T2 host 2001:400::f00::2 2001:400::f00::9 key testing123
  timeout 2
- > aaa tacacs+-server T3 host "tac.aos.com" key testing123
Release History

Release 7.1.1; command was introduced.
Release 7.3.1; vrf-name parameter added.
Release 8.3.1; prompt-key parameter added.
Release 8.6R1; salt and hash-salt parameters added.
Release 8.7 R3; support for IPv6 added for TACACS+

Related Commands

show aaa server  Displays information about AAA servers.

aaa authentication  Specifies the AAA servers to be used for Authenticated Switch Access.

aaa accounting session  Specifies the accounting servers to be used for Authenticated Switch Access.

MIB Objects

aaaServerTable
   aaasName
   aaasProtocol
   aaasHostName
   aaasIpAddress
   aaasIpv6Address
   aaasHostName2
   aaasIpAddress2
   aaasIpv6Address2
   aaasTacacsKey
   aaasTimeout
   aaasTacacsPort
   aaasVrfName
   aaasRadSalt
   aaasRadSaltHash
aaa tacacs command-authorization

Configures a command based authorization in TACACS+ server for authenticated switch.

aaa tacacs command-authorization {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Disable command based authorization in TACACS+ server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disable command based authorization. This enables partition-management family based authorization in TACACS+ server.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is applicable only for CLI commands.
- If this command is enabled, then in the TACACS+ server the authorization of every command executed on the switch is command based. CLI commands executed on the switch are sent for authorization to the TACACS+ server along with-mode of operation (read or read-write). After authorization, the server will send the response message to the TACACS+ client.
- If the command is disabled, then in the TACACS+ server the authorization is partition-management family based.
- Use show configuration snapshot aaa command to view the configuration details of this command.

Examples

- `aaa tacacs command-authorization enable`
- `aaa tacacs command-authorization disable`

Release History

Release 8.3.1; command was introduced.
Related Commands

**show aaa server**
Displays information about AAA servers.

MIB Objects

alaAaaAuthConfig
alaAaaTacacsServerCmdAuthorization
aaa ldap-server

Configures or modifies an LDAP server for Authenticated Switch Access.

**aaa ldap-server** server_name host {hostname | ip_address | ipv6_address} [hostname2 | ip_address2 | ipv6_address2] dn dn_name {password super_password | prompt-password}[salt salt | hash-salt] [base search_base] [retransmit retries] [timeout seconds] [ssl | no ssl] [port port] [vrf-name name]

**no aaa ldap-server** server_name

---

**Syntax Definitions**

- **server_name**
  - The name of the LDAP server.

- **hostname**
  - The host name (DNS name) of the primary LDAP server. The host name or IP address is required when creating a server.

- **ip_address** | **ipv6_address**
  - The IPv4 or IPv6 address of the primary LDAP server.

- **hostname2**
  - The host name (DNS name) of the backup LDAP server.

- **ip_address2** | **ipv6_address2**
  - The IPv4 or IPv6 address of a backup host for the LDAP server.

- **dn_name**
  - The super-user or administrative distinguished name in the format recognized by the LDAP-enabled directory servers. For example: `cn=manager`. Must be different from the `search-base` name and must be in a format supported by the server. Required when creating a new server.

- **super_password**
  - The super-user password recognized by the LDAP-enabled directory servers. The password may be clear text or hexadecimal format. Required when creating a new server.

- **prompt-password**
  - This option enters the super-user password in an obscured format rather than as clear text. When this option is selected, press the Enter key. A password prompt appears asking for the super-user password. Re-enter the password and only if both the passwords match, the command is accepted. Password provided in this mode is not displayed on the CLI as text.

- **salt**
  - The input given through ‘salt’ will be used to add randomness to the encryption of the key. The maximum length of the salt is 15 characters and must be in clear text format. By default, the system time will be taken as default salt value.

- **hash-salt**
  - The salt value for which the input must be in an encrypted format. The maximum length of the hash-salt should not exceed 64 characters.

- **search_base**
  - The search base recognized by the LDAP-enabled directory servers. For example, `o=company` or `c=country`. Must be different from the `dn_name`. Required when creating a new server.

- **retries**
  - The number of retries the switch makes to the LDAP server to authenticate a user before trying the backup server.

- **seconds**
  - The timeout in seconds for server replies to authentication requests from the switch.
AAA Commands

aaa ldap-server

ssl
Enables Transport Layer Security (TLS) between the switch and the LDAP server.

no ssl
Disables Transport Layer Security (TLS) between the switch and the LDAP server.

port
The port number for the primary LDAP server and any backup server. Must match the port number configured on the server.

name
The name of the VRF to be used to access the server.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>389 (SSL disabled) 636 (SSL enabled)</td>
</tr>
<tr>
<td>retries</td>
<td>3</td>
</tr>
<tr>
<td>seconds</td>
<td>2</td>
</tr>
<tr>
<td>ssl</td>
<td>no ssl</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The dn_name must be different from the search_base name.
- Use the no form of the command to remove an LDAP server from the configuration. Only one server may be removed at a time.
- The port number configured on the switch must match the port number configured for the server.
- If ‘salt’ and ‘hash-salt’ parameters are configured at a time, hash-salt value is given priority over salt.
- The special character ‘!’ and pure integers will not be accepted as a valid input for both salt and hashsalt.
- If you want to provide special characters in salt value, give it in between "" double quotes.
- The input given through ‘salt’ and ‘hash-salt’ is encrypted and will be displayed as ‘hash-salt’ in 'show configuration snapshot' command.
- Backward compatibility for ‘salt’ and ‘hash-salt’ is not supported. In case of an accidental downgrade, boot.cfg error is generated for that particular configuration, and re-configuration is required.
- LDAP server can be configured on any VRF instance or the default VRF instance. However, all the LDAP servers must reside on the same VRF instance.
For IPV6 address, IPV6 LDAP host and interface must be configured in the switch.

**Examples**

-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager password tpub base c=us retransmit 4
-> aaa ldap-server omnivista host 1.2.3.4 dn "cn=DirMgr, o=alcatel.com" password somepass base "ou=People, o=alcatel.com" vrf-name ldap_vrf
-> no aaa ldap-server topanga5

-> aaa ldap-server topanga5 host 10.10.3.4 dn cn=manager prompt-password base c=us retransmit 4
Enter Password: *******
Confirm Password: *******

-> aaa ldap-server L1 host 10.10.10.5 dn cn=manager password tpub base c=us salt mysalt

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.1; `vrf-name` parameter added.
Release 8.3.1; `prompt-password` parameter added.
Release 8.6R1; `salt` and `hash-salt` parameters added.
Release 8.7 R1; IPv6 support added.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show aaa server</code></td>
<td>Displays information about AAA servers.</td>
</tr>
<tr>
<td><code>aaa authentication</code></td>
<td>Specifies the AAA servers to be used for authenticated switch access.</td>
</tr>
<tr>
<td><code>aaa accounting session</code></td>
<td>Specifies the accounting servers to be used for Authenticated Switch Access.</td>
</tr>
</tbody>
</table>
**MIB Objects**

aaaServerTable
  aaasProtocol
  aaasHostName
  aaasIpAddress
  aaasIp6Address
  aaasHostName2
  aaasIpAddress2
  aaasIp6Address2
  aaasLdapPort
  aaasLdapDn
  aaasLdapPasswd
  aaasLdapSearchBase
  aaasLdapServType
  aaasRetries
  aaasTimeout
  aaasLdapEnableSsl
  aaasVrfName
  aaasLdapSaltHash
  aaasLdapPasswdHash
**system fips admin-state**

Enable or disable the Federal Information Processing Standards (FIPS) mode on the switch.

```
system fips admin-state {enable | disable}
```

### Syntax Definitions

- **enable** | **disable**
  
  Enables or disables the FIPS mode.

### Defaults

By default, the FIPS mode is disabled on the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enabling or disabling FIPS mode takes effect only after a switch reboot. The FIPS mode configuration is persistent across reboots.
- When FIPS mode is disabled, all other existing cryptographic algorithms will be supported.
- A FIPS supported client is required to access the switch in FIPS enabled mode. For example, Absolute Telnet.
- Other unsecured management interfaces, such as Telnet or FTP, have to be manually disabled after FIPS mode is enabled to achieve a completely secure device.

### Examples

```
-> system fips admin-state enable
WARNING: FIPS Admin State only becomes Operational after write memory and reload
```

```
-> system fips admin-state disable
WARNING: FIPS Admin State only becomes Operational after write memory and reload
```

### Release History

Release 8.1.1; command introduced.
Related Commands

show system fips

Show the configured and running status of the FIPS mode on the Switch.

MIB Objects

systemFipsAdminState
aaa authentication

Configures the interface for Authenticated Switch Access and specifies the server(s) to be used. This type of authentication gives users access to manage the switch.

`aaa authentication {console | telnet | ftp | http | snmp | ssh | default} server1 [server2...] [local]`

`no aaa authentication {console | telnet | ftp | http | snmp | ssh | default}`

**Syntax Definitions**

- `console` Configures Authenticated Switch Access through the console port.
- `telnet` Configures Authenticated Switch Access for any port used for Telnet.
- `ftp` Configures Authenticated Switch Access for any port used for FTP.
- `http` Configures Authenticated Switch Access for any port used for Web-based management.
- `snmp` Configures Authenticated Switch Access for any port used for SNMP.
- `ssh` Configures Authenticated Switch Access for any port used for Secure Shell.
- `default` Configures Authenticated Switch Access for any port using any service (`telnet`, `ftp`, etc.). Note that SNMP access is enabled only if an LDAP or local server is specified with the command.
- `server1` The name of the authentication server used for Authenticated Switch Access. At least one server is required. The server may be a RADIUS, TACACS+, LDAP, or the local user database. RADIUS, TACACS+, and LDAP server names are set up through the `aaa radius-server`, `aaa tacacs+-server`, and `aaa ldap-server` commands.
- `server2...` The names of backup servers for Authenticated Switch Access. Up to 3 backups may be specified (including `local`). These backups are only used if `server1` becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.
- `local` Specifies that the local user database will be a backup for the authentication servers. If you want to use the local user database as the only authentication server, specify `local` for `server1`.

**Defaults**

- At switch startup, Authenticated Switch Access is available through console port via the local database. Authentication for other management interfaces (Telnet, FTP, etc.) is disabled.
- The default user on the switch is `admin`, and `switch` is the password.
- Remote authentication is not supported on secondary CMMs or Slave chassis. Use local authentication on secondary CMMs and Slave chassis.
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The server type may be RADIUS, TACACS+, LDAP, or the local user database. Up to 4 servers may be configured for an interface type; at least one is required. Each server name should be separated by a space.
- The switch uses only the first available server in the list to check for user information. For example, if server1 is not available, the switch will poll server2. If user information is not found on the first available server, the authentication request will fail.
- RADIUS, TACACS+, and LDAP servers may each have an additional backup specified through the aaa radius-server, aaa tacacs+-server, and aaa ldap-server commands.
- If the local switch database will be used as the only authentication server, specify local for server1. If local is specified as a backup server, it should be entered last in the list of servers. The local user database is always available if the switch is up.
- Only LDAP or the local database may be used for authenticated SNMP management.
- If Secure Shell (ssh) is enabled, Telnet and FTP should be disabled.

Examples

- => aaa authentication telnet pubs1
- => no aaa authentication telnet
- => aaa authentication default pubs2 pubs3

Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **aaa radius-server**
  Configures or modifies a RADIUS server for Authenticated Switch Access.

- **aaa ldap-server**
  Configures or modifies an LDAP server for Authenticated Switch Access.

- **user**
  Configures user information for the local database on the switch.

- **show aaa server**
  Displays information about servers configured for Authenticated Switch Access.

**MIB Objects**

- **aaaAuthSATable**
  - aaatsInterface
  - aaasName
  - aaatsName1
  - aaatsName2
  - aaatsName3
  - aaatsName4
aaa console admin-only

Enables or disables the user restriction for all users except the user “admin” from accessing the switch through the secure console session.

```
aaa console admin-only {enable | disable}
```

**Syntax Definitions**

- `enable` - Restricts all users from accessing the switch through the secure console session except the user “admin”. Only user “admin” can access the switch through the secure console session.
- `disable` - Disables the user restrictions.

**Defaults**

By default, console admin-only is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enable this feature to restrict all users except user “admin” from accessing the switch through the secure console session.

**Examples**

```
-> aaa console admin-only enable
-> aaa console admin-only disable
```

**Release History**

Release 8.3.1 R02; command was introduced.

**Related Commands**

- `user` - Configures user information for the local database on the switch.

**MIB Objects**

- `aaaAsaAccessConsoleAdminOnly`
aaa authentication default

Sets the authenticated switch access type to the default server setting.

```
aaa authentication {console | telnet | ftp | http | snmp | ssh} default
```

### Syntax Definitions

- **console**
  - Configures the default Authenticated Switch Access server setting for the console port.
- **telnet**
  - Configures the default Authenticated Switch Access server setting for Telnet.
- **ftp**
  - Configures the default Authenticated Switch Access server setting for FTP.
- **http**
  - Configures the default Authenticated Switch Access server setting for Web-based management.
- **snmp**
  - Configures the default Authenticated Switch Access server setting for any port used for SNMP.
- **ssh**
  - Configures the default Authenticated Switch Access server setting for any port used for Secure Shell.

### Defaults

By default, the default Authenticated Switch Access server setting does not include any servers.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `aaa authentication` command to set the default servers.

### Examples

```
-> aaa authentication telnet default
-> aaa authentication default default
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

**aaa radius-server**
Configures or modifies a RADIUS server for Authenticated Switch Access.

**aaa tacacs+-server**
Configures or modifies an LDAP server for Authenticated Switch Access.

**user**
Configures user information for the local database on the switch.

**show aaa server**
Displays information about servers configured for Authenticated Switch Access.

MIB Objects

aaaAuthSATable
- aaatsName1
- aaatsName2
- aaatsName3
- aaatsName4
aaa accounting session

Configures an accounting server or servers for authenticated switch sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

```
aaa accounting session server1 [server2...] [local]
no accounting session
```

Syntax Definitions

- **server1**: The name of the RADIUS, TACACS+, or LDAP server used for accounting of authenticated switch sessions. At least one server is required. RADIUS, TACACS+, and LDAP server names are set up through the `aaa radius-server`, `aaa tacacs+-server`, and `aaa ldap-server` commands.

- **server2...**: The names of backup servers. Up to 3 backups may be specified (including `local`); each server name should be separated by a space. These backups are only used if `server1` becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.

- **local**: Local accounting is done through the Switching Logging feature on the switch.

Defaults

Accounting is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of the command to disable accounting for Authenticated Switch Access.

- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.

- The servers may be RADIUS, TACACS+, LDAP servers, and/or the local Switch Logging facility.

- If `local` is specified as `server1`, the switch will only use the local Switching Logging facility for accounting.

- If `local` is specified as a backup, it should be entered last in the list of servers. The Switch Logging facility is always available if the switch is up.
The switch uses *only the first available server* in the list for accounting. For example, if `server1` is not available, the switch will use `server2`.

- RADIUS, TACACS+, and LDAP servers may each have an additional backup specified through the `aaa radius-server`, `aaa tacacs+-server`, and `aaa ldap-server` commands.

**Examples**

```
-> aaa accounting session ldap1 radius2 local
-> no aaa accounting session
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show aaa accounting` Displays information about accounting servers configured for Authenticated Switch Access.

**MIB Objects**

aaAcctsTable

- aaacsName1
- aaacsName2
- aaacsName3
- aaacsName4
aaa accounting command

Enables or disables the server for command accounting. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

```
aaa accounting command server1 [server2...] [local]

no accounting command
```

**Syntax Definitions**

- `server1`: The name of the TACACS+ server used for command accounting. At least one server is required. TACACS+ server names are set up through the `aaa tacacs+-server` commands.

- `server2...`: The names of TACACS+ backup servers. Up to 3 backups may be specified; each server name should be separated by a space. These backups are only used if `server1` becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.

- `local`: Local accounting is done through the Switching Logging feature on the switch.

**Defaults**

Accounting is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to disable command accounting.

- Up to 4 accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.

- The servers can be only TACACS+ servers.

- The switch uses `only the first available server` in the list for accounting. For example, if `server1` is not available, the switch will use `server2`.

- TACACS+ server may each have an additional backup specified through the `aaa tacacs+-server` command.
**Examples**

-> aaa accounting command tacacs1 tacacs2 tacacs3
-> no aaa accounting command

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

**show aaa accounting**  
Displays information about accounting servers configured for Authenticated Switch Access.

**MIB Objects**

`aaaAcctCmdTable`

- `aaacmdSrvName1`
- `aaacmdSrvName2`
- `aaacmdSrvName3`
- `aaacmdSrvName4`
aaa device-authentication

Configures the switch to use RADIUS servers for 802.1X, MAC, and Captive Portal device authentication.

aaa device-authentication {802.1x | mac | captive-portal} server1 [server2] [server3] [server4]

no device-authentication {802.1x | mac | captive-portal}

Syntax Definitions

802.1x  Use the specified RADIUS server to authenticate 802.1X users.
mac     Use the specified RADIUS server for MAC authentication.
captive-portal Use the specified RADIUS server for Captive Portal authentication.
server1 The name of the RADIUS authentication server to use for the specified type of authentication. (Note that only RADIUS servers are supported for these types of authentication.) At least one server is required. RADIUS server names are configured through the aaa radius-server command.

server2...server4 The names of backup servers used for authentication. Up to 3 backups may be specified; include a space between each server name. These backups are only used if server1 becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the authentication server.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove a RADIUS server assignment for a specific authentication type.

- Up to 4 RADIUS servers (total) may be specified. At least one server is required. Each server name should be separated by a space.

- The switch uses only the first available server in the list to check for user information. For example, if server1 is not available, the switch will poll server2. If user information is not found on the first available server, the authentication request will fail.
• RADIUS servers may each have an additional backup specified through the `aaa radius-server` command.

• Configuring the RADIUS servers to use for 802.1X, MAC, and Captive Portal authentication is required to support authentication and classification of devices connected to Universal Network Profile (UNP) ports.

**Examples**

```
-> aaa device-authentication 802.1x rad1
-> aaa device-authentication 802.1x rad1 rad2
-> no aaa device-authentication 802.1x

-> aaa device-authentication mac rad1
-> aaa device-authentication mac rad1 rad2
-> no aaa device authentication mac

-> aaa device-authentication captive-portal rad1
-> aaa device-authentication captive-portal rad1 rad2
-> no aaa device-authentication captive-portal
```

**Release History**

Release 7.2.1; command was introduced.
Release 7.3.4; **802.1x** parameter added.
Release 8.1.1; **captive-portal** parameter added.

**Related Commands**

- `aaa radius-server` Configures or modifies a RADIUS server for authenticated switch access or device authentication.
- `unp port-type` Enables or disables UNP port-based access control on a port.
- `show aaa device-authentication` Displays a list of RADIUS servers assigned to provide 802.1X or MAC authentication.

**MIB Objects**

AaaAuthDATable
  - `aaaDaName1`
  - `aaaDaName2`
  - `aaaDaName3`
  - `aaaDaName4`
aaa accounting

Configures RADIUS server accounting or local Switch Logging (syslog) accounting for 802.1X, MAC, and Captive Portal authenticated device sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

```
aaa accounting {802.1x | mac | captive-portal} {server1 [server2...] | syslog ip_address [port udp_port]}
no accounting {802.1x | mac | captive-portal}
```

Syntax Definitions

- **802.1x** Enables the specified RADIUS or syslog server to log accounting of 802.1X authenticated sessions.
- **mac** Enables the specified RADIUS or syslog server to log accounting for MAC authenticated sessions.
- **captive-portal** Enables the specified RADIUS or syslog server to log accounting for Captive Portal authenticated sessions.
- **server1** The name of the RADIUS server used for accounting of authenticated switch sessions. At least one server is required. RADIUS server names are configured through the `aaa radius-server` command.
- **server2...** The names of backup servers. Up to 3 backups may be specified; each server name should be separated by a space. These backups are only used if `server1` becomes unavailable. They are polled in the order they are listed in this command. The first available server becomes the accounting server.
- **ip_address** The IP network address for syslog accounting.
- **udp_port** The UDP port number for syslog accounting.

Defaults

By default, no RADIUS server or syslog accounting is configured for the switch.

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp_port</td>
<td>514</td>
</tr>
</tbody>
</table>
```

Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```
Usage Guidelines

- Use the **no** form of the command to disable accounting for device authentication sessions.
- Up to 4 RADIUS accounting servers (total) may be specified. At least one server is required. Each server name should be separated by a space.
- The switch uses **only the first available server** in the list for accounting. For example, if server1 is not available, the switch will use server2.
- Accounting with the local syslog facility is not allowed if RADIUS accounting is already configured. In other words, configure either RADIUS or syslog accounting.
- RADIUS servers may each have an additional backup specified through the **aaa radius-server** command.

Examples

```
-> aaa accounting 802.1x rad1
-> aaa accounting 802.1x rad1 rad2 rad3 rad4
-> aaa accounting 802.1x syslog 10.135.67.99 port 8000
-> no aaa accounting 802.1x

-> aaa accounting mac rad1
-> aaa accounting mac rad1 rad2
-> aaa accounting mac syslog 10.135.67.99 port 8000
-> no aaa accounting mac

-> aaa accounting captive-portal rad1
-> aaa accounting captive-portal rad1 rad2 rad3
-> aaa accounting captive-portal syslog 10.135.67.99 port 8000
-> no aaa accounting captive-portal
```

Release History

Release 8.1.1; command was introduced.

Related Commands

- `show aaa accounting` Displays the accounting server configuration for the switch.

MIB Objects

```
aaaAcctDATable
  aaacdInterface
  aaacdName1
  aaacdName2
  aaacdName3
  aaacdName4
  aaacdSyslogIPAddrType
  aaacdSyslogIPAddr
  aaacdSyslogUdpPort
```
aaa accounting radius calling-station-id

Configures the RADIUS Calling-Station-Id attribute for the specified accounting session type.

```
aaa accounting {802.1x | mac | captive-portal} radius calling-station-id {mac-address | ip-address}
```

**Syntax Definitions**

- **802.1x**  
  Configures the attribute for 802.1X accounting sessions.
- **mac**  
  Configures the attribute for MAC accounting sessions.
- **captive-portal**  
  Configures the attribute for Captive Portal accounting sessions.
- **mac-address**  
  Sets the Calling Station ID to the MAC address of the user.
- **ip-address**  
  Sets the Calling Station ID to the IP address of the user.

**Defaults**

By default, the RADIUS Calling-Station-Id attribute value is set to the MAC address of the user.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Configuring the Calling-Station-Id attribute is not allowed if the accounting server configuration is set to use local Switch Logging (syslog) for the specified accounting session type (802.1x, MAC, or Captive Portal).
- The Calling Station ID attribute is defined in a RADIUS Accounting-Request message that is sent to the RADIUS accounting server.

**Examples**

- `-> aaa accounting 802.1x radius calling-station-id ip-address`
- `-> no aaa accounting 802.1x radius calling-station-id ip-address`
- `-> aaa accounting 802.1x radius calling-station-id mac-address`

- `-> aaa accounting mac radius calling-station-id ip-address`
- `-> no aaa accounting mac radius calling-station-id ip-address`
- `-> aaa accounting mac radius calling-station-id mac-address`

- `-> aaa accounting captive-portal radius calling-station-id ip-address`
- `-> no aaa accounting onex radius calling-station-id ip-address`
- `-> aaa accounting captive-portal radius calling-station-id mac-address`
**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `show aaa accounting` Displays the AAA accounting configuration.

**MIB Objects**

- `aaaAcctDATable`
  - `aaacdInterface`
  - `aaacdCallingStationId`
aaa 802.1x re-authentication

Configures the automatic re-authentication of authenticated 802.1X users.

`aaa 802.1x re-authentication {enable | disable | interval seconds | trust-radius {enable | disable}}`

**Syntax Definitions**

- **enable** Enables re-authentication of 802.1X users.
- **disable** Disables re-authentication of 802.1X users.
- **seconds** The amount of time the switch waits before triggering re-authentication of 802.1X users. The valid range is 600–7200 seconds.
- **trust-radius enable** Directs the switch to use the Session-Timeout attribute value for the re-authentication time interval. This attribute is returned from the RADIUS server in an Accept-Accept message.
- **trust-radius disable** Directs the switch to use the locally configured re-authentication time interval value.

**Defaults**

By default, 802.1X re-authentication is disabled for the switch. When re-authentication is enabled, the following default values apply:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>3600</td>
</tr>
<tr>
<td>trust-radius enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The re-authentication time interval is triggered when 802.1X re-authentication is enabled.
- When the re-authentication time interval is changed, the new value does not apply to existing authenticated 802.1X users until the user is flushed out or when the user is authenticated again. Any new 802.1X users are re-authenticated based on the current time interval setting.
- When the trust RADIUS option is enabled, the Session-Timeout attribute value received from the RADIUS server overrides the locally configured value for the switch.
AAA profile settings for 802.1x re-authentication take precedence over global 802.1x re-authentication settings configured with this command. For example, if the global trust RADIUS option is enabled and the AAA profile trust RADIUS option is disabled (the default), the trust RADIUS status is disabled on the UNP port when the AAA profile is assigned to that port.

**Examples**

-> aaa 802.1x re-authentication enable
-> aaa 802.1x re-authentication enable interval 7200
-> aaa 802.1x re-authentication enable trust-radius enable
-> aaa 802.1x re-authentication enable interval 7200 trust-radius enable
-> aaa 802.1x re-authentication interval 7200 trust-radius disable
-> aaa 802.1x re-authentication disable

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

*show aaa config* Displays the global AAA parameter configuration for 802.1X sessions.

**MIB Objects**

alaAaaAuthConfig
alaAaaOnexReAuthStatus
alaAaaOnexReAuthIntrvl
alaAaaOnexReAuthTrustRadStatus
aaa interim-interval

Configures the amount of time between each interim accounting update for any given session.

```
aaa {802.1x | mac | captive-portal} interim-interval seconds [trust-radius {enable | disable}]
```

### Syntax Definitions

- **802.1x**
  - Configures the interim interval value for 802.1X accounting sessions.

- **mac**
  - Configures the interim interval value for MAC accounting sessions.

- **captive-portal**
  - Configures the interim interval value for Captive Portal accounting sessions.

- **seconds**
  - The amount of time between each interim accounting update. The valid range is 60–1200 seconds.

- **trust-radius enable**
  - Directs the switch to use the Acct-Interim-Interval attribute value for the interim time interval. This attribute is returned from the RADIUS server in an Accept-Accept message.

- **trust-radius disable**
  - Directs the switch to use the locally configured interim time interval value.

### Defaults

By default, the accounting interim interval value is set to 600 seconds.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>trust-radius enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When the trust RADIUS option is enabled, the accounting interim interval value received from the RADIUS server overrides the locally configured value for the switch.

- When the accounting interim interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.

### Examples

```
-> aaa 802.1x interim-interval 1200
-> aaa 802.1x interim-interval 1200 trust-radius enable
```
AAA Commands

-> aaa 802.1x interim-interval 1200 trust-radius disable
-> aaa mac interim-interval 1200
-> aaa mac interim-interval 1200 trust-radius enable
-> aaa mac interim-interval 1200 trust-radius disable

-> aaa captive-portal interim-interval 1200
-> aaa captive-portal interim-interval 1200 trust-radius enable
-> aaa captive-portal interim-interval 1200 trust-radius disable

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- **show aaa config**
  Displays the global AAA parameter configuration for device authentication and accounting sessions.

**MIB Objects**

alaAaaAuthConfig
  - alaAaaOnexIntrmIntvl
  - alaAaaOnexIntmIntvlTrstRadSts
  - alaAaaMacIntrmIntvl
  - alaAaaMacIntmIntvlTrstRadStatus
  - alaAaaCpIntrmIntvl
  - alaAaaCpIntmIntvlTrstRadStatus
aaa session-timeout

Configures whether or not an authenticated user is automatically logged out of the network based on a session timeout value.

`aaa {mac | captive-portal} session-timeout {enable | disable} [interval seconds] [trust-radius {enable | disable}]`

### Syntax Definitions

- **mac**: Configures the session timeout parameter for authenticated MAC users.
- **captive-portal**: Configures the session timeout parameter for authenticated Captive Portal users.
- **session-timeout enable**: Enables the session timeout timer for authenticated user sessions.
- **session-timeout disable**: Disables the session timeout timer for authenticated user sessions.
- **seconds**: The session timeout value. The valid range is 300–172800 seconds.
- **trust-radius enable**: Directs the switch to use the Session-Timeout attribute returned from the RADIUS server in an Accept-Accept message.
- **trust-radius disable**: Directs the switch to use the locally configured timeout interval value.

### Defaults

By default, the session timer is disabled for the switch.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>43200 seconds</td>
</tr>
<tr>
<td></td>
<td>(12 hours)</td>
</tr>
<tr>
<td>`trust-radius enable</td>
<td>disable`</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The session timeout parameter is configurable only for MAC and Captive Portal authentication sessions. When 802.1x re-authentication is enabled, the session timeout is set to 43200 seconds by default.
- The timeout interval is triggered when the session timeout parameter is enabled for the switch.
• When the trust RADIUS option is enabled, the timeout interval value received from the RADIUS server overrides the locally configured value for the switch.

• When the session timeout interval is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.

• When the session timeout value is reached, the authenticated users are logged out and the MAC address for each logged out user device is flushed.

Examples

-> aaa mac session-timeout enable interval 13000
-> aaa mac session-timeout enable interval 14000 trust-radius enable
-> aaa mac session-timeout disable

-> aaa captive-portal session-timeout enable interval 13000
-> aaa captive-portal session-timeout enable interval 14000 trust-radius enable
-> aaa captive-portal session-timeout disable

Release History
Release 8.1.1; command was introduced.

Related Commands

show aaa config Displays the global AAA parameter configuration for device authentication and accounting sessions.

MIB Objects

alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
alaAaaAuthConfig
aaa session console

Enables or disables switch access through the console port of the switch.

```
aaa session console {enable | disable}
```

**Syntax Definitions**

- `enable`: Enables the switch access through the console port through the CLI shell.
- `disable`: Disables the switch access through the console port through the CLI shell.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- It is recommended to create a back-up of the configuration file before using this command. Contact customer support to recover the switch.

- Before disabling the CLI console shell, configuration for telnet or SSH access with proper user privilege must be made.

- When the CLI console shell is disabled, the switch log output to the console is also disabled.

- When the CLI console shell is disabled, the switch can be accessed through SSH or telnet or WebView session.

- The command can be stored to the configuration file using `write memory`.

- If the console access is disabled through configuration (on both working and certified directory) and the telnet/SSH/WebView session is also not available to the switch, contact customer support to recover the switch.

**Note.** Deleting the configuration file will also delete the other configurations. Hence, it is recommended to create a back-up of the configuration file before deleting the configuration file.
• In a virtual chassis, the command must be used only on the master chassis; the console on master and all slaves will be disabled/enabled accordingly.

**Examples**

-> session console disable
-> session console enable

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

*show aaa session console config*  Displays Session Manager information, such as banner file name, session timeout value, and default prompt value.

**MIB Objects**

`alaAaaConsoleAccessConfig
alaAaaConsoleAccessAdminState`
aaa inactivity-logout

Configures whether or not an authenticated user is automatically logged out of the network after a specific period of inactivity.

```
aaa {mac | captive-portal} inactivity-logout {enable | disable} [interval seconds]
```

**Syntax Definitions**

- **mac**: Configures the inactivity logout timer for authenticated MAC users.
- **captive-portal**: Configures the inactivity logout timer for authenticated Captive Portal users.
- **enable**: Enables the inactivity logout timer for the specified authentication type.
- **disable**: Disables the inactivity logout timer for the specified authentication type.
- **seconds**: The inactivity logout time. The valid range is 60–1200 seconds, or enter 0 to indicate that an authenticated user should never be logged out.

**Defaults**

By default, the inactivity logout timer is disabled for the switch.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>600 seconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The inactivity logout timer is configurable only for MAC and Captive Portal authentication sessions.
- The timer is triggered when the inactivity logout parameter is enabled for the switch.
- Make sure the configured inactivity logout time is set to a value greater than the MAC address aging time for the switch.
- If a specific time is configured for the inactivity logout timer, the user is not logged out of the network even if the MAC address for the user device ages out before the inactivity logout timer value expires.
- Setting the inactivity logout time to zero helps prevent silent devices from getting automatically logged out; the silent device will always remain logged in.
- When the inactivity logout time is changed, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
• If a user undergoes MAC authentication and then secondary Captive Portal authentication, the higher of the two inactivity logout timer values is applied to the device.

**Examples**

```bash
-> aaa mac inactivity-logout enable
-> aaa mac inactivity-logout enable interval 600
-> aaa mac inactivity-logout enable interval 0
-> aaa mac inactivity-logout disable

-> aaa captive-portal inactivity-logout enable
-> aaa captive-portal inactivity-logout enable interval 600
-> aaa captive-portal inactivity-logout enable interval 0
-> aaa captive-portal inactivity-logout disable
```

**Release History**

Release 8.1.1; command was introduced.
Release 8.4.1.R02; setting the inactivity logout time to zero is supported (user is never logged out).

**Related Commands**

`show aaa config` Displays the global AAA parameter configuration for device authentication and accounting sessions.

**MIB Objects**

```plaintext
alaAaaAuthConfig
  alaAaaMacInActLogoutStatus
  alaAaaMacInActLogoutIntrvl
  alaAaaCpInActLogoutStatus
  alaAaaCpInActLogoutIntrvl
```
aaa radius nas-port-id

Configures the RADIUS client NAS-Port attribute for authentication and accounting sessions.

aaa radius nas-port-id {user-string string | default}

### Syntax Definitions

- **string**: A text string (up to 31 characters) used to define a NAS-Port identifier for the NAS-Port attribute.
- **default**: Sets the NAS-Port attribute value to the chassis/slot/port of the user.

### Defaults

By default, the NAS-Port attribute is set to the user port (chassis/slot/port).

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The NAS-Port attribute value specified with this command is used in Account-Request messages and in Accounting-Request messages.

### Examples

- `-> aaa radius nas-port-id default`
- `-> aaa radius nas-port-id user-string nasport`

### Release History

Release 8.1.1; command was introduced.

### Related Commands

- **show aaa radius config**: Displays the global RADIUS client attribute configuration.

### MIB Objects

- `alaAaaClientAttrGroup`  
- `alaAaaRadNasPortId`
aaa radius nas-identifier

Configures the RADIUS client NAS-Identifier attribute for authentication and accounting sessions.

aaa radius nas-identifier {user-string string | default}

**Syntax Definitions**

- **string**
  - A text string (up to 31 characters) used to identify the switch (RADIUS client) in the NAS-Identifier attribute.

- **default**
  - Sets the NAS-Identifier attribute to the system name of the switch.

**Defaults**

By default, the NAS-Identifier attribute is set to the system name of the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The NAS-Identifier attribute value specified with this command is used in both Account-Request and Accounting-Request messages.

**Examples**

- `-> aaa radius nas-identifier default`
- `-> aaa radius nas-identifier user-string os6860`

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `show aaa radius config` Displays the global RADIUS client attribute configuration.

**MIB Objects**

alaAaaClientAttrGroup
  - `alaAaaRadNasIdentifier`
aaa radius nas-ip-address

Configure the RADIUS client NAS IP address attribute for the outgoing RADIUS packets.

`aaa radius nas-ip-address {default | local-ip [ip_address]}`

**Syntax Definitions**

- **default**
  Sets the NAS IP address attribute value to the source IP address of the interface used to send the RADIUS packet. In OmniVista Cirrus it will be the VPN IP address.

- **local-ip**
  Sets the NAS IP address attribute value with the DHCP-Client interface IP address as the device identifier.

- **ip_address**
  The IPv4 address for NAS IP address attribute in RADIUS packets.

**Defaults**

By default, the value of NAS IP address is default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The NAS IP address attribute value configured will be used in all Authentication-Request messages and in Accounting-Request messages.

- If the Local IP is configured without the optional IP address, then the NAS IP address attribute value will be the DHCP-Client interface IP address.

- If there is no DHCP IP address configured on the switch, then NAS IP address attribute will contain the IP address as per the default behavior.

- If Local IP option is configured with an IP address, then this configured IP address value will be used in the NAS IP address attribute.

**Examples**

- `-> aaa radius nas-ip-address default`
- `-> aaa radius nas-ip-address local-ip`
**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

*show aaa radius config*  
Displays the global AAA attribute values.

**MIB Objects**

alaAaaClientAttrGroup  
  alaAaaRadNasIpAddressMode  
  alaAaaRadNasIpAddressType  
  alaAaaRadNasIpAddress
aaa radius mac-format

Configures the MAC address format to use in the specified RADIUS client attributes.

```
aaa radius mac-format {username | password | calling-station-id | called-station-id} delimiter {char | none} case {uppercase | lowercase}
```

### Syntax Definitions

- **username**: Configures the MAC address format for the User-Name attribute.
- **password**: Configures the MAC address format for the User-Password attribute.
- **calling-station-id**: Configures the MAC address format for the Calling-Station-Id attribute.
- **called-station-id**: Configures the MAC address format for the Called-Station-Id attribute.
- **char**: The delimiter character to use to separate the octets within a MAC address. The valid characters are a space (" "), a hyphen ("-"), or a colon (":"). For example, “e8:e7:32:a4:63:23”, “e8-e7-32-a4-63-23”, or “e8:e7:32:a4:63:23”.
- **none**: No delimiter is used in the MAC address format.
- **uppercase**: Uses uppercase characters in the MAC address format.
- **lowercase**: Uses lowercase characters in the MAC address format.

### Defaults

By default, no delimiter is used and the MAC address characters are in uppercase.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The MAC address format configured for the User-Name and User-Password attributes is only applied for MAC authentication and accounting, where these attributes are set to the MAC address of the user. The configured format is not applied for 802.1X or Captive Portal authentication and accounting.
- The MAC address format configured for the Called-Station-Id and Calling-Station-Id attributes is applied for MAC, 802.1X, and Captive Portal authentication and accounting sessions when these attributes are set to a MAC address value.
- The Called-Station-Id attribute is set to the base MAC address of the switch.
- The Calling-Station-ID attribute is configurable and can be set to the MAC address or IP address of the user.
Examples

-> aaa radius mac-format username delimiter none case lowercase
-> aaa radius mac-format username delimiter ":" case lowercase

-> aaa radius mac-format password delimiter none case lowercase
-> aaa radius mac-format password delimiter ":" case lowercase
-> aaa radius mac-format calling-station-id delimiter none case lowercase
-> aaa radius mac-format calling-station-id delimiter ":" case lowercase

-> aaa radius mac-format called-station-id delimiter none case lowercase
-> aaa radius mac-format called-station-id delimiter ":" case lowercase

Release History

Release 8.1.1; command was introduced.

Related Commands

aaa accounting radius calling-station-id
Sets the Calling-Station-Id attribute to the MAC address or IP address of the user for accounting sessions.

show aaa radius config
Displays the global RADIUS client attribute configuration.

MIB Objects

alaAaaRadiusClientGlobalAttr
alaAaaRadiusUserNameDelimiter
alaAaaRadiusUserNameCase
alaAaaRadiusPasswordDelimiter
alaAaaRadiusPasswordCase
alaAaaRadCallInStnIdDelim
alaAaaRadiusCallingStationIdCase
alaAaaRadCallIdStnIdDelim
alaAaaRadiusCalledStationIdCase
aaa profile

Configures an AAA profile that is used to define and apply specific AAA parameter values to Universal Network Profile (UNP) Edge ports, link aggregates, or an Access Guardian Captive Portal profile. This section describes the base command (aaa profile profile_name) along with the other command keywords that are used to configure AAA parameter values that are applied when the profile is assigned to a UNP port or link aggregate.

`aaa profile profile_name`

[device-authentication {802.1x | mac | captive-portal} server1 [server2] [server3] [server4]]

[accounting {802.1x | mac | captive-portal} {server1 [server2... | syslog ip_address}

[accounting {802.1x | mac | captive-portal} radius calling-station-id {mac-address | ip-address}]

[802.1x re-authentication {enable | disable} [interval seconds] [trust-radius {enable | disable}]]

[802.1x | mac | captive-portal] interim-interval seconds [trust-radius {enable | disable}]

[mac | captive-portal] session-timeout {enable | disable} [interval seconds] [trust-radius {enable | disable}]

[mac | captive-portal] inactivity-logout {enable | disable} [interval seconds]

[radius nas-port-id {user-string string | default}]

[radius nas-identifier {user-string string | default}]

[radius nas-ip-address {default | local-ip [ip_address]}]

[radius mac-format {username | password | calling-station-id | called-station-id} delimiter {char | none} case {uppercase | lowercase}]

no aaa profile profile_name

---

Syntax Definitions

`profile_name`  The name to associate with the AAA configuration profile.

Defaults

The AAA profile parameters are set to the same default values that are set when the explicit AAA command is used to configure the parameter value. See the show aaa profile command output example in the “Examples” section of this command page to determine default values for AAA profile parameters.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to remove the AAA profile from the switch configuration.

- Creating the template name with the base command (`aaa profile profile_name`) is required before attempting to configure profile parameter values.

- When an AAA profile is assigned to a UNP port, the parameter values defined in the profile will override any existing global AAA configuration for users authenticating on that port.

- When an AAA profile is assigned to a Captive Portal profile, the parameters values defined in the AAA profile will override any existing global AAA configuration for users authenticated through the Captive Portal profile configuration.

- For more information about specific AAA parameter values, refer to the following explicit AAA configuration commands for each profile parameter option:

<table>
<thead>
<tr>
<th>AAA Profile Parameter</th>
<th>Explicit Port Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>[device-authentication {802.1x</td>
<td>mac</td>
</tr>
<tr>
<td>[accounting {802.1x</td>
<td>mac</td>
</tr>
<tr>
<td>[radius device-authentication 802.1x re-authentication {enable</td>
<td>disable} [interval seconds] [trust-radius {enable</td>
</tr>
<tr>
<td>[mac</td>
<td>captive-portal] interim-interval seconds [trust-radius {enable</td>
</tr>
<tr>
<td>[mac</td>
<td>captive-portal] session-timeout {enable</td>
</tr>
<tr>
<td>[mac</td>
<td>captive-portal] inactivity-logout {enable</td>
</tr>
<tr>
<td>[radius nas-port-id {user-string string</td>
<td>default]}</td>
</tr>
<tr>
<td>[radius nas-identifier {user-string string</td>
<td>default]}</td>
</tr>
<tr>
<td>[radius nas-ip-address {default</td>
<td>local-ip ip_address}]</td>
</tr>
<tr>
<td>[radius mac-format {username</td>
<td>password</td>
</tr>
</tbody>
</table>

**Examples**

- `-> aaa profile prof1`
- `-> no aaa profile prof1`
- `-> aaa profile ap-1 device-authentication mac rad1 rad2`
- `-> aaa profile ap-1 device-authentication 802.1x serv1 serv2 serv3 serv4`
- `-> aaa profile ap-2 device-authentication captive-portal rad3 rad4`
- `-> no aaa profile ap-2 device-authentication captive-portal`
-> aaa profile ap-1 accounting 802.1x rad1 rad2 rad3
-> aaa profile ap-1 accounting mac rad1 rad2
-> aaa profile ap-1 accounting captive-portal syslog 10.135.67.99 port 8000
-> no aaa profile ap-1 accounting captive-portal

-> aaa profile ap-1 802.1x re-authentication enable trust-radius enable
-> aaa profile ap-1 802.1x re-authentication enable interval 700
-> aaa profile ap-1 802.1x re-authentication interval 700 trust-radius disable
-> aaa profile ap-1 802.1x re-authentication disable
-> aaa profile ap-1 mac inactivity-logout enable
-> aaa profile ap-1 mac inactivity-logout enable interval 600
-> aaa profile ap-1 mac inactivity-logout disable

-> aaa profile ap-1 captive-portal inactivity-logout enable
-> aaa profile ap-1 captive-portal inactivity-logout enable interval 600
-> aaa profile ap-1 captive-portal inactivity-logout disable

-> aaa profile abc radius nas-ip-address default
-> aaa profile abc radius nas-ip-address local-ip
-> aaa profile abc radius nas-ip-address local-ip 192.168.1.1

The following show aaa profile command output example shows the default values applied when the AAA profile is created:

-> show aaa profile ap-2
AAA profile name = ap-2
Authentication type = mac
    Session Timeout:
        Status = disable,
        Interval (sec) = 43200,
        Trust Radius = disable

    Inactivity Timeout:
        Status = disable,
        Interval (sec) = 600

    Accounting Interim:
        Interval (sec) = 600,
        Trust Radius = disable

Authentication type = 802.1x
    Re-Authentication Timeout:
        Status = disable,
        Interval (sec) = 3600,
        Trust Radius = disable

    Accounting Interim:
        Interval (sec) = 600,
        Trust Radius = disable

Authentication type = captive-portal
    Session Timeout:
        Status = disable,
        Interval (sec) = 43200,
        Trust Radius = disable

    Inactivity Timeout:
        Status = disable,
        Interval (sec) = 600
AAA Commands

AAA Commands aaa profile

Accounting Interim:
   Interval (sec)  = 600,
   Trust Radius   = disable
RADIUS client attributes:
   NAS port id     = default,
   NAS identifier  = default,
   NAS IP address  = default,
   MAC format delimiter:
      Username      = none, UserNameCase = uppercase,
      Password      = none, PasswordCase = uppercase,
      calling station id = none, ClgStaIdCase = uppercase,
      called station id = none, CldStaIdCase = uppercase

Release History

Release 8.1.1; command was introduced.
Release 8.5R4; radius nas-ip-address parameter added.

Related Commands

unp aaa-profile Assigns an AAA profile to a UNP Edge port.
captive-portal-profile Assigns an AAA profile to a Captive Portal profile.
show aaa profile Displays the AAA profile configuration.
**MIB Objects**

- `alaAaaProfTable`
- `alaAaaProfOnexReAuthSts`
- `alaAaaProfOnexReAuthIntrvl`
- `alaAaaProfOnexReAuthTrstRadSts`
- `alaAaaProfOnexIntmIntrvl`
- `alaAaaProfOnexIntmIntrvlTrstRadSts`
- `alaAaaProfMacIntmIntrvl`
- `alaAaaProfMacIntmIntrvlTrstRadSts`
- `alaAaaProfMacSessTimeoutIntrvl`
- `alaAaaProfMacSessTimeoutTrstRadSts`
- `alaAaaProfMacInActLogoutIntrvl`
- `alaAaaProfMacInActLogoutTrstRadSts`
- `alaAaaProfCpSessTimeoutIntrvl`
- `alaAaaProfCpSessTimeoutTrstRadSts`
- `alaAaaProfCpInActLogoutIntrvl`
- `alaAaaProfCpInActLogoutTrstRadSts`
- `alaAaaProfCpImtrmIntrvl`
- `alaAaaProfCpImtrmIntrvlTrstRadSts`
- `alaAaaProfRadNasPortId`
- `alaAaaProfRadNasIdentifier`
- `alaAaaProfRadUserNameDelim`
- `alaAaaProfRadPasswordDelim`
- `alaAaaProfRadCallnStnIdDelim`
- `alaAaaProfRadCalldStnIdDelim`
- `alaAaaProfRadUserNameCase`
- `alaAaaProfRadPasswordCase`
- `alaAaaProfRadCallnStnIdCase`
- `alaAaaProfRadCalldStnIdCase`
- `alaAaaRadNasIpAddressMode`
- `alaAaaRadNasIpAddressType`
- `alaAaaRadNasIpAddress`
**user**

Configures or modifies user entries in the local user database. Use the `no` form of the command to remove the user from the local database.

`user username`

*{password password | password-prompt}*

*expiration {day | date}*

*read-only | read-write [families... | domains... | all | none | all-except [families | domains.... | | macsec]]*

*no snmp | no auth | sha | md5 | sha+des | md5+des | sha+aes | sha224 | sha256 | sha384 | sha224+aes | sha256+aes | sha384+aes]*

*console-only {enable | disable}*

*[priv-password password | prompt-priv-password]*

`no user username`

**Syntax Definitions**

*username*  
The name of the user. Used for logging into the switch. Required to create a new user entry or for modifying a user. Maximum 63 characters.

*password*  
The user’s password in clear text or hexadecimal (corresponding to encrypted form). Required to create a new user entry. Maximum 30 characters.

*password-prompt*  
This option allows to enter the password in a obscured format rather than as clear text. Select this option with the ‘user’ command to configure the password for the user. When this option is selected, a password prompt appears and the password can be provided. Password needs to be re-entered, and only if both the passwords match, command is accepted. The password provided in this mode is not displayed on the CLI as text.

*day*  
The number of days before this user’s current password expires. The range is 1 to 150 days.

*date*  
The date (in the format *mm/dd/yyyy*) that the user’s current password will expire.

*read-only*  
Specifies that the user will have read-only access to the switch.

*read-write*  
Specifies that the user will have read-write access to the switch.

*families*  
Determines the command families available to the user on the switch. Each command family should be separated by a space. Command families are subsets of domains.

*domains*  
Determines the command domains available to the user on the switch. Each domain should be separated by a space.

*all*  
Specifies that all command families and domains are available to the user.

*none*  
Specifies that no command families or domains are available to the user.

*all-except*  
Specifies that functional privilege for families or domains followed by 'all-except' are disabled to the user.
By default, if a user is created without indicating the read and write privileges and SNMP access, the user will be given privileges based on the default user account. The default user account may be modified.

**Defaults**

- By default, if a user is created without indicating the read and write privileges and SNMP access, the user will be given privileges based on the default user account. The default user account may be modified.
By default, the password will be encrypted using SHA for all non SNMP users.

For SNMP users without authentication, password will be encrypted with SHA.

For SNMP users with authentication, it will be encrypted with the authentication method set for the user. If user is created with MD5, then it will be still encrypted with MD5.

Users created with SHA2 authentication algorithm cannot be used for SNMP authentication.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- At least one user with SHA/MD5 authentication and/or DES encryption must be configured on the switch for SNMPv3 communication with OmniVista.

- Note that the exclamation point ‘!’ is not a valid password character. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk. For example, password **123456** is allowed; password ******** is not allowed.

- Some special characters are interpreted as a Linux shell variable by the switch when being used in a password. They can still be used in a password but they must be escaped (\') or the entire password enclosed in single quotes. For example, to use the ‘$’ as part of a password the following should be entered:

  -> user test password test\$1234

  or

  -> user test password ‘test$1234’

  these passwords will be interpreted as test$1234.

- An alternative method is to use the password-prompt parameter when using special characters in a password. The password-prompt parameter exits the Linux shell and special characters are no longer interpreted as shell variables. The following characters are the majority of characters considered special characters by the switch [" " (white space), $, "", \#, [, ], <, >, ;, {, }, 0, ~, ].

- A password expiration for the user’s current password may be configured with the expiration option. However, if the password is changed, or the global password expiration setting is configured with the user password-expiration command, the user’s password expiration will be configured with the global expiration setting.

- When modifying a user’s SNMP access, the user password must be re-entered (or a new one configured). This is required because the hash algorithm used to save the password in the switch depends on the SNMP authentication level.
At initial startup, the default user on the switch is **admin** with a password of **switch**. The switch will not recreate this user at any successive startup as long as there exists at least one user defined with write access to all commands. (Note that if password expiration is configured for the **admin** user, or configured globally through the **user password-expiration** command, when the **admin** user’s password expires, the **admin** user will have access only through the console port.)

New users or updated user settings are saved automatically.

After changing the **priv-password** it could take up to 5 minutes to become effective.

The **priv-password** token is accepted only when SNMP level with encryption is configured for the user. If SNMP level with encryption is not selected and **priv-password** is configured, then CLI command is rejected with error.

If **priv-password** is not configured for the user with encryption SNMP level, then the user password parameter is used for **priv-password** (both for authentication/encryption).

Password policy is not applicable for the new optional parameter **priv-password**.

For authenticating switch access through other access types such as telnet, FTP, SSH the existing user password will be used irrespective of whether **priv-password** is configured or not.

When the SNMP level for an existing user with **priv-password** configured is changed from one encryption level to another encryption level, then the previously configured **priv-password** will not be used with the new SNMP level. **Priv-password** needs to be configured again when SNMP level is changed for an existing user.

Only users with MACsec read-write privilege can configure MACsec. Use ‘**user**’ command to enable MACsec read-write permissions to the users. The privilege can be configured by family or by security domain.

**Examples**

```
-> user techpubs password writer_pass read-only config
-> user techpubs password-prompt
Enter Password: *******
Confirm Password: *******

-> user techpubs password writer_pass read-write all sha256

The following example creates a user with read-write privileges for all families except aaa.
-> user techpubs password writer_pass read-write all-except aaa
-> no user techpubs

-> user snmpv3user password pass1pass1 priv-password priv1priv1 read-write all sha+aes

-> user snmpv3user password pass1pass1 prompt-priv-password
Enter Priv-Password: *********
Confirm Priv-Password: *********
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1; **password-prompt**, **all-except**, **priv-password**, **prompt-priv-password** parameter added, **sha224** and **sha256** algorithm support added.
Release 8.7 R01; Support for sha384, sha224+aes, sha256+aes, and sha384+aes added.
Release 8.9R1; macsec keyword added.

Related Commands

password
  Configures the current user’s password.
show user
  Displays information about users configured in the local database.

MIB Objects

aaaUserTable
  aaauPassword
  aaauReadRight
  aaauWriteRight
  aaauSnmpLevel
  aaauSnmpAuthKey
  aaauPasswordExpirationDate
password

Configures the current user’s password.

password

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the snapshot command is used to capture the switch configuration, the text of the password is not displayed in the file. Instead an authentication key is included in the file.

- A new password cannot be identical to the current password; it cannot be identical to any of the three passwords that preceded the current password.

- Note that the exclamation point (!) is not a valid password character. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk. For example, password **123456** is allowed; password ******** is not allowed.

- Password settings are saved automatically.

Examples

-> password
enter old password: ********
enter new password: *********
reenter new password: *********
->

Release History

Release 7.1.1; command was introduced.
Related Commands

user

Configures entries in the local user database. May be used by a system administrator to change any user’s password in addition to configuring user privileges.

MIB Objects

aaaUserTable

aaaPassword

aaaOldPassword
super-password

Configures the password to grant more privileges to the other non-secureadmin user in the secureadmin mode.

`enable super-password`

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900 X48C4E/V48C8/</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The super-password can be set only by the secureadmin user.
- If the `snapshot` command is used to capture the switch configuration, the text of the password is not displayed in the file. Instead an authentication key is included in the file.
- A new password cannot be identical to the current password; it cannot be identical to any of the three passwords that preceded the current password.
- Note that the exclamation point (!) is not a valid password character. In addition, specifying an asterisk (*) as one or more characters in a password is allowed as long as every character is not an asterisk. For example, `password **123456**` is allowed; `password ********` is not allowed.
- Password settings are saved automatically.

Examples

`-> enable super-password`

`enter super-password: ********`

`reenter super-password: ********`

Release History

Release 8.8R1; command was introduced.
Related Commands

**user**

Configures entries in the local user database. May be used by a system administrator to change any user’s password in addition to configuring user privileges.

MIB Objects

<table>
<thead>
<tr>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaaUserTable</td>
</tr>
<tr>
<td>alaAaaSuperPassword</td>
</tr>
</tbody>
</table>
user password-size min

Configures the minimum number of characters required when configuring a user password.

user password-size min size

**Syntax Definitions**

- **size**: The number of characters required when configuring a user password through the `password` command or when setting up a user password through the `user` command. The range is 1 to 30 characters. For the superadmin user the range is 1 to 20 characters.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>size</td>
<td>8</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `->` user password-size min 9

**Release History**

Release 7.1.1; command was introduced.
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>user</strong></td>
<td>Configures entries in the local user database. May be used by a system</td>
</tr>
<tr>
<td></td>
<td>administrator to change any user’s password in addition to configuring</td>
</tr>
<tr>
<td></td>
<td>user privileges.</td>
</tr>
<tr>
<td><strong>show user password-policy</strong></td>
<td>Displays the global password policy configuration for the switch.</td>
</tr>
</tbody>
</table>

## MIB Objects

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaaAsaConfig</td>
<td></td>
</tr>
<tr>
<td>aaaAsaPasswordSizeMin</td>
<td></td>
</tr>
</tbody>
</table>
**user password-expiration**

Configures an expiration date for all user passwords stored locally on the switch or disables password expiration.

```
user password-expiration {day | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>day</code></td>
<td>The number of days before locally configured user passwords will expire. The range is 1 to 150 days.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables password expiration for users configured locally on the switch.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>`day</td>
<td>disable`</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The **user password-expiration** command sets a default password expiration for users configured locally on the switch.

- Password expiration may be configured on a per-user basis through the **user** command; the user setting overrides the **user password-expiration** setting until the user password is changed or the **user password-expiration** command is entered again.

### Examples

```
-> user password-expiration 2
-> user password-expiration disable
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

**user**  
Configures entries in the local user database. May be used by a system administrator to change any user’s password in addition to configuring user privileges.

**show user password-policy**  
Displays the global password policy configuration for the switch.

**MIB Objects**

- `aaaAsaConfig`
  - `aaaAsaDefaultPasswordExpirationInDays`
**user allow-ssh**

This command enables or disables SSH access to the switch to a specific user.

```bash
user username allow-ssh {enable | disable}
```

**Syntax Definitions**

- `username` The name of the user. Used for logging into the switch. Required to create a new user entry or for modifying a user. Maximum 63 characters.
- `enable` Enable SSH access to the switch.
- `disable` Disables SSH access to the switch.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the SSH access option is disabled, user cannot access the switch through SSH.

**Examples**

```bash
-> user test allow-ssh enable
-> user test allow-ssh disable
```

**Release History**

Release 8.8R2; command introduced.
Related Commands

**user**
Configures entries in the local user database. May be used by a system administrator to change any user’s password in addition to configuring user privileges.

**show user**
Displays the global password policy configuration for the switch.

MIB Objects

aaaUserTable
aaauAllowSsh
user password-policy cannot-contain-username

Specifies whether or not a user can configure a password that contains the username for the account.

user password-policy cannot-contain-username {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Does not allow the password to contain the username.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Allows the password to contain the username.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The status of this function is specified as part of a global password policy that is applied to all passwords when they are created or modified.
- When this function is enabled, a check is done at the time the password is created or modified to ensure that the username is not specified as part of the password text.

Examples

- user password-policy cannot-contain-username enable
- user password-policy cannot-contain-username disable

Release History

Release 7.1.1; command was introduced.

Related Commands

- show user password-policy Displays the global password policy configuration for the switch.

MIB Objects

aaaAsaConfig
aaaAsaPasswordContainUserName
**user password-policy cannot-contain-consecutive-characters**

Specifies whether or not a user can configure a password that contains consecutive characters or three or more consecutive identical characters.

**user password-policy cannot-contain-consecutive-characters {enable | disable}**

---

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>disable</td>
<td></td>
</tr>
</tbody>
</table>

Does not allow the password to contain the consecutive-characters.

Allows the password to contain the consecutive-characters.

---

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- The status of this function is specified as part of a global password policy that is applied to all passwords when they are created or modified.

- When this function is enabled, a check is done at the time the password is created or modified to ensure that the password does not contain consecutive-characters or three or more identical characters.

- In secureadmin mode by default this is enabled.

---

### Examples

- `-> user password-policy cannot-contain-consecutive-characters enable`
- `-> user password-policy cannot-contain-consecutive-characters disable`

---

### Release History

Release 8.9R2; command was introduced.
Related Commands

show user password-policy  Displays the global password policy configuration for the switch.

MIB Objects

aaaAsaConfig
  aaaAsaPasswordContainConsecutiveCharacters
user password-policy min-uppercase

Configures the minimum number of uppercase English characters required for a valid password.

user password-policy min-uppercase number

Syntax Definitions

number The minimum number of uppercase characters. The valid range is 0–7.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>1</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900
    V72/C32 | 6900 | 9900
| 6900 | 9900 |
Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes
```

Usage Guidelines

- Specify 0 with this command to disable the minimum uppercase character requirement.
- The minimum number of uppercase characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

```
-> user password-policy min-uppercase 2
-> user password-policy min-uppercase 0
```

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy Displays the global password policy configuration for the switch.

MIB Objects

aaaAsaConfig
aaaAsaPasswordMinUpperCase
user password-policy min-lowercase

Configures the minimum number of lowercase English characters required for a valid password.

Syntax:

```
user password-policy min-lowercase number
```

**Syntax Definitions**

`number` The minimum number of uppercase characters. The valid range is 0–7.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify 0 with this command to disable the minimum lowercase character requirement.
- The minimum number of lowercase characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

**Examples**

```
-> user password-policy min-lowercase 2
-> user password-policy min-lowercase 0
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show user password-policy` Displays the global password policy configuration for the switch.

**MIB Objects**

- `aaaAsaConfig`  
  - `aaaAsaPasswordMinLowerCase`
user password-policy min-digit

Configures the minimum number of base-10 digits required for a valid password.

user password-policy min-digit number

Syntax Definitions

number The minimum number of uppercase characters. The valid range is 0–7.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>1</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specify **0** with this command to disable the minimum number of digits requirement.
- The minimum number of digits requirement is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

- -> user password-policy min-digit 2
- -> user password-policy min-digit 0

Release History

Release 7.1.1; command was introduced.

Related Commands

show user password-policy Displays the global password policy configuration for the switch.

MIB Objects

aaaAsaConfig
  aaaAsaPasswordMinDigit
user password-policy min-nonalpha

Configures the minimum number of non-alphanumeric characters (symbols) required for a valid password.

user password-policy min-nonalpha number

---

Syntax Definitions

number The minimum number of non-alphanumeric characters. The valid range is 0–7.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>1</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specify 0 with this command to disable the minimum non-alphanumeric character requirement.
- The minimum number of non-alphanumeric characters is specified as part of a global password policy that is applied to all passwords when they are created or modified.

Examples

- `-> user password-policy min-nonalpha 2`
- `-> user password-policy min-nonalpha 0`

Release History

Release 7.1.1; command was introduced.

Related Commands

- show user password-policy Displays the global password policy configuration for the switch.
MIB Objects

aaaAsaConfig
  aaaAsaPasswordMinNonAlpha
**user password-history**

Configures the maximum number of old passwords to retain in the password history.

```
user password-history number
```

---

**Syntax Definitions**

`number` The maximum number of old passwords to retain. The range is 0–24.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>4</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Specify 0 with this command to disable the password history function.
- The user is prevented from specifying any passwords that are recorded in the password history and fall within the range configured through this command.
- The password history value is specified as part of a global password policy that is applied to all passwords when they are created or modified.

**Examples**

- `-> user password-history 2`
- `-> user password-history 0`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show user password-policy` Displays the global password policy configuration for the switch.
**MIB Objects**

aaaAsaConfig

aaaAsaPasswordHistory
**user password-min-age**

Configures the minimum number of days during which a user is prevented from changing a password.

```
user password-min-age days
```

### Syntax Definitions

```
days
```

The number of days to use as the minimum age of the password. The range is 0–150.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>days</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Specify 0 with this command to disable the minimum number of days requirement.
- Configure the minimum age of a password with a value that is less than the value configured for the password expiration.
- The password minimum age value is specified as part of a global password policy that is applied to all passwords when they are created or modified.

### Examples

```
-> user password-min-age 7
-> user password-min-age 0
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show user password-policy` Displays the global password policy configuration for the switch.
MIB Objects

aaaAsaConfig
  aaaAsaPasswordMinAge
user lockout-window

Configures a moving period of time (observation window) during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts. The number of failed login attempts is decremented by the number of failed attempts that age beyond the observation window time period.

user lockout-window minutes

Syntax Definitions

minutes The number of minutes the observation window remains active. The range is 0–99999.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>0</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command is only available to the admin user because the admin user account is the only account protected from any type of lockout attempt.
- Specify 0 with this command to disable the observation window function. This means that failed login attempts will never age out; the number of failed attempts is never decremented.
- Do not configure an observation window time period that is greater than the lockout duration time period.
- If the number of failed login attempts exceeds the number of failed attempts allowed before the observation window time expires, then the user account is locked out of the switch.
- The observation window time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved automatically.

Examples

-> user lockout-window 500
-> user lockout-window 0

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user lockout-duration</td>
<td>Configures the amount of time a user account remains locked out of the switch.</td>
</tr>
<tr>
<td>user lockout-threshold</td>
<td>Configures the number of failed password attempts allowed before the user account is locked out of the switch.</td>
</tr>
<tr>
<td>user lockout unlock</td>
<td>Manually locks or unlocks a user account on the switch.</td>
</tr>
<tr>
<td>show user lockout-setting</td>
<td>Displays the global user lockout settings for the switch.</td>
</tr>
</tbody>
</table>

**MIB Objects**

aaaAsaConfig
  aaaAsaLockoutWindow
**user lockout-threshold**

Configures the number of failed password login attempts allowed during a certain period of time (observation window). If the number of failed attempts equals the lockout threshold number before the observation window period expires, the user account is locked out.

`user lockout-threshold number`

### Syntax Definitions

- **number**: The number of failed login attempts allowed. The range is 0–999.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is only available to the `admin` user because the `admin` user account is the only account protected from any type of lockout attempt.
- If the lockout threshold is set to zero (the default), there is no limit to the number of failed login attempts allowed.
- A user account remains locked out for the length of the lockout duration time period; at the end of this time, the account is automatically unlocked.
- If the lockout duration time period is set to zero, only the `admin` user or a user with read/write AAA privileges can unlock a locked user account. An account is unlocked by changing the user account password or with the `user lockout unlock` command.
- The lockout threshold time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved *automatically*; that is, these settings do not require the `write memory`, `reload slot`, or `configuration snapshot` command to save user settings over a reboot.

### Examples

```
-> user lockout-threshold 3
```
user lockout-threshold 0

Release History
Release 7.1.1; command was introduced.

Related Commands
- **user lockout-window**
  Configures a window of time during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts.
- **user lockout-duration**
  Configures the length of time a user account remains locked out of the switch.
- **user lockout unlock**
  Manually locks or unlocks a user account on the switch.
- **show user lockout-setting**
  Displays the global user lockout settings for the switch.

MIB Objects
- **aaaAsaConfig**
  - **aaaAsaLockoutThreshold**
**user lockout-duration**

Configures the length of time a user account remains locked out of the switch. At the end of this time period, the user account is automatically unlocked.

**user lockout-duration** minutes

---

**Syntax Definitions**

*minutes* The number of minutes the user account remains locked out. The range is 0–99999.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command is only available to the *admin* user because the *admin* user account is the only account protected from any type of lockout attempt.
- Note that if the lockout duration time period is set to zero (the default), then locked user accounts are never automatically unlocked.
- Only the *admin* user or a user with read/write AAA privileges can unlock a locked user account when the lockout duration time is set to zero. An account is unlocked by changing the user password or with the *user lockout unlock* command.
- Do not configure a lockout duration time period that is less than the amount of time configured for the observation window.
- The lockout duration time period is a global lockout setting that is applied to all passwords configured on the switch.
- Lockout settings are saved automatically; that is, these settings do not require the *write memory*, *reload slot*, or *configuration snapshot* command to save user settings over a reboot.

**Examples**

```plaintext
-> user lockout-duration 60
```
-> user lockout-duration 0

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **user lockout-window**
  Configures a window of time during which failed login attempts are counted to determine if the number of failed attempts has exceeded the number of allowed attempts.

- **user lockout-threshold**
  Configures the number of failed password attempts allowed before the user account is locked out of the switch.

- **user lockout unlock**
  Manually locks or unlocks a user account on the switch.

- **show user lockout-setting**
  Displays the global user lockout settings for the switch.

**MIB Objects**

- **aaaAsaConfig**
  - **aaaAsaLockoutDuration**
**user lockout unlock**

Manually locks or unlocks a user account on the switch.

`user username {lockout | unlock}`

### Syntax Definitions

- **username**: The username of the account to lock or unlock.
- **lockout**: Locks the user account out of the switch.
- **unlock**: Unlocks a locked user account.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is only available to the **admin** user or a user with read/write AAA privileges.
- The **admin** user account is protected from any type of lockout attempt.
- User lockouts and unlocks are saved automatically.

### Examples

```
-> user j_smith lockout
-> user j_smith unlock
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **show user**: Displays information about all users or a particular user configured in the local user database on the switch.
- **show user lockout-setting**: Displays the global user lockout settings for the switch.
MIB Objects

aaaUserTable
  aaaPasswordLockoutEnable
**show aaa server**

Displays information about a particular AAA server or AAA servers.

```bash
show aaa server [server_name]
```

### Syntax Definitions

- **server_name**: The server name, which is defined through the `aaa radius-server`, `aaa tacacs+-server`, or `aaa ldap-server` commands.

### Defaults

- N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If a server name is not included with this command, information for all of the servers is displayed.

### Examples

```bash
-> show aaa server
Server name = ldap2
    Server type = LDAP,
    Host name 1 = ors40535,
    Retry number = 3,
    Timeout (sec) = 2,
    Port = 389,
    Domain name = manager,
    Search base = c=us,
    VRF = default
Server name = rad1
    Server type = RADIUS,
    IP Address 1 = 10.10.2.1,
    IP Address 2 = 10.10.3.5,
    Retry number = 3,
    Timeout (sec) = 2,
    Authentication port = 1645,
    Accounting port = 1646,
    SSL enable = TRUE,
    VRF = default
    Health Check = ENABLED,
    Primary Server:
```
AAA Commands

show aaa server

Status      = DOWN,
Uptime      = -,
Downtime    = -,
Down to UP transitions = 0,
Backup Server :
    Status      = DOWN,
    Uptime      = -,
    Downtime    = -,
    Down to UP transitions = 0
Server name = Tpub1
    Server type          = TACACS+,
    IP Address 1         = 10.10.5.1,
    Port                 = 3,
    Timeout (sec)        = 2,
    Encryption enabled   = no
    VRF                   = default

-> show aaa server rad1
Server name = rad1
    Server type = RADIUS,
    IP Address 1 = 10.10.2.1,
    IP Address 2 = 10.10.3.5,
    Retry number = 3,
    Timeout (sec) = 2,
    Authentication port = 1645,
    Accounting port = 1646
    SSL enable          = TRUE,
    VRF                   = default
    Health Check           = ENABLED,
Primary Server:
    Status      = DOWN,
    Uptime      = -,
    Downtime    = -,
    Down to UP transitions = 0,
Backup Server :
    Status      = DOWN,
    Uptime      = -,
    Downtime    = -,
    Down to UP transitions = 0

-> show aaa server ldap2
Server name = ldap2
    Server type = LDAP,
    Host name 1 = ors40535,
    Retry number = 3,
    Timeout (in sec) = 2,
    Port = 389,
    Domain name = manager,
    Search base = c=us,
    VRF                   = default

output definitions

<table>
<thead>
<tr>
<th>Server name</th>
<th>The name of the server. A RADIUS, TACACS+ or LDAP server name is defined through the aaa radius-server, aaa tacacs+-server, and aaa ldap-server commands respectively.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server type</td>
<td>The type of server (LDAP, TACACS+, or RADIUS).</td>
</tr>
</tbody>
</table>
AAA Commands show aaa server

**Release History**

Release 7.1.1; command was introduced.
Release 8.4.1; **SSL enable** output field added for RADIUS server.
Release 8.5R4; **Health Check**, **Primary Server**, and **Backup Server** fields added for RADIUS server.

**Related Commands**

- **aaa radius-server** Configures or modifies a RADIUS server for Authenticated Switch Access.
- **aaa ldap-server** Configures or modifies an LDAP server for Authenticated Switch Access.
- **aaa tacacs+-server** Configures or modifies a TACACS+ server for Authenticated Switch Access.
- **aaa radius-server health-check** Defines the RADIUS server health check configuration for a specific RADIUS server.
- **show aaa radius health-check-config** Displays the RADIUS server health check configuration.

<table>
<thead>
<tr>
<th><strong>output definitions</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host name</strong></td>
<td>The name of the primary LDAP, TACACS+, or RADIUS host.</td>
</tr>
<tr>
<td><strong>IP address</strong></td>
<td>The IP address of the server.</td>
</tr>
<tr>
<td><strong>Retry number</strong></td>
<td>The number of retries the switch makes to authenticate a user before trying the backup server.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The timeout for server replies to authentication requests.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port number for the primary LDAP or TACACS+ server.</td>
</tr>
<tr>
<td><strong>Encryption enabled</strong></td>
<td>The status of the encryption.</td>
</tr>
<tr>
<td><strong>Domain name</strong></td>
<td>The super-user or administrative distinguished name in the format recognized by the LDAP-enabled directory servers.</td>
</tr>
<tr>
<td><strong>Search base</strong></td>
<td>The search base recognized by the LDAP-enabled directory servers.</td>
</tr>
<tr>
<td><strong>Authentication port</strong></td>
<td>The UDP destination port for authentication requests.</td>
</tr>
<tr>
<td><strong>Accounting port</strong></td>
<td>The UDP destination port for accounting requests.</td>
</tr>
<tr>
<td><strong>SSL enable</strong></td>
<td>The SSL enable field is displayed for the RADIUS server only when the SSL is enabled for RADIUS server.</td>
</tr>
<tr>
<td><strong>VRF</strong></td>
<td>Name of the VRF associated with the server.</td>
</tr>
<tr>
<td><strong>Health Check</strong></td>
<td>Whether a health check session is enabled or disabled for the RADIUS server.</td>
</tr>
<tr>
<td><strong>Primary Server</strong></td>
<td>The operational status, up time, down time, and the number of transitions from down to up for the primary RADIUS server. This field displays information gathered when RADIUS health check is enabled for the server.</td>
</tr>
<tr>
<td><strong>Backup Server</strong></td>
<td>The operational status, up time, down time, and the number of transitions from down to up for the back-up RADIUS server. This field displays information gathered when RADIUS health check is enabled for the server.</td>
</tr>
</tbody>
</table>
MIB Objects

aaaServerTable
  aaasName
  aaasHostName
  aaasIpAddress
  aaasIpv6Address
  aaasHostName2
  aaasIpAddress2
  aaasIpv6Address2
  aaasRadKey
  aaasRetries
  aaasTimout
  aaasRadAuthPort
  aaasRadAcctPort
  aaasProtocol
  aaasTacacsKey
  aaasTacacsPort
  aaasLdapPort
  aaasLdapDn
  aaasLdapPasswd
  aaasLdapSearchBase
  aaasLdapServType
  aaasLdapEnableSsl
  aaasRadEnableSsl
  aaasVRFName
  aaasRadHealthCheck
show aaa server statistics

Displays the authorization, authentication, accounting, and BYOD statistics for the specified RADIUS server.

show aaa server server_name statistics

Syntax Definitions

server_name
The name of the RADIUS server for which statistics will be displayed.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command applies only to RADIUS servers known to the switch (servers are identified through the aaa radius-server command).

- All statistics displayed for authorization, authentication, and accounting are displayed as an aggregate of the primary and back-up RADIUS server; separate statistics are not displayed for the primary server and the back-up server.

- Use the aaa radius-server clear-statistics command to reset all the statistics counters to zero.

Examples

-> show aaa server rad2 statistics
Statistics for rad2:
Authorization:
Total No of Access-Request : 2
Total No of Access-Response : 2
Total No of Timedout Request : 0
Min RTT of Access Req/Res  usec: 938
Avg RTT of Access Req/Res  usec: 1087
Max RTT of Access Req/Res  usec: 1237
Last RTT of Access Req/Res usec: 1237
Authentication:
Total No of Access-Request : 1
Total No of Access-Response : 1
Total No of Access-Accept : 1
Total No of Access-Reject : 0
AAA Commands

show aaa server statistics

Total No of Access-Challenge : 0
Total No of Timedout Request  : 0
Min RTT of Access Req/Res   usec: 1176
Avg RTT of Access Req/Res   usec: 1176
Max RTT of Access Req/Res   usec: 1176
Last RTT of Access Req/Res  usec: 1176

Accounting:
Total No of Acct-Request     : 2
Total No of Acct-Response    : 2
Total No of Timedout Request : 0
Min RTT of Acct Req/Res     usec: 76657
Avg RTT of Acct Req/Res     usec: 80182
Max RTT of Acct Req/Res     usec: 83708
Last RTT of Acct Req/Res    usec: 83708

BYOD:
Total No of COA Request      : 0
Total No of COA ACK Sent     : 0
Total No of COA NACK Sent    : 0
Total No of DM Request       : 0
Total No of DM ACK Sent      : 0
Total No of DM NACK Sent     : 0

Time of last statistics clear : Thu Feb  1 18:09:06 2018

-> show aaa server auth-serv1 statistics
ERROR: Statistics are supported only for RADIUS servers

output definitions

<table>
<thead>
<tr>
<th>Authorization</th>
<th>The statistics information displayed for authorization.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total No of Access-Request</td>
<td>The total number of authorization access requests sent to the server.</td>
</tr>
<tr>
<td>Total No of Access-Response</td>
<td>The total number of authorization access responses received from the server.</td>
</tr>
<tr>
<td>Total No of Timedout Request</td>
<td>The total number of authorization access requests that timed out.</td>
</tr>
<tr>
<td>Min RTT of Access Req/Res</td>
<td>The minimum RTT of authorization access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Avg RTT of Access Req/Res</td>
<td>The average RTT of authorization access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Max RTT of Access Req/Res</td>
<td>The maximum RTT of authorization access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Last RTT of Access Req/Res</td>
<td>The last RTT of authorization access requests or responses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication</th>
<th>The statistics information displayed for authentication.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total No of Access-Request</td>
<td>The total number of authentication access requests sent to the server.</td>
</tr>
<tr>
<td>Total No of Access-Response</td>
<td>The total number of authentication access responses received from the server.</td>
</tr>
<tr>
<td>Total No of Access-Accept</td>
<td>The total number of authentication access accepts received from the server.</td>
</tr>
<tr>
<td>Total No of Access-Reject</td>
<td>The total number of authentication access rejects received from the server.</td>
</tr>
<tr>
<td>Total No of Access-Challenge</td>
<td>The total number of authentication access challenges received from the server.</td>
</tr>
</tbody>
</table>
### output definitions

<table>
<thead>
<tr>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total No of Timedout Request</td>
<td>The total number of authentication access requests that timed out.</td>
</tr>
<tr>
<td>Min RTT of Access Req/Res</td>
<td>The minimum RTT of authentication access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Avg RTT of Access Req/Res</td>
<td>The average RTT of authentication access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Max RTT of Access Req/Res</td>
<td>The maximum RTT of authentication access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Last RTT of Access Req/Res</td>
<td>The last RTT of authentication access requests or responses.</td>
</tr>
<tr>
<td>Accounting</td>
<td>The statistics information displayed for accounting.</td>
</tr>
<tr>
<td>Total No of Acct -Request</td>
<td>The total number of accounting access requests sent to the server.</td>
</tr>
<tr>
<td>Total No of Acct -Response</td>
<td>The total number of accounting access responses received from the server.</td>
</tr>
<tr>
<td>Total No of Timedout Request</td>
<td>The total number of accounting access requests that timed out.</td>
</tr>
<tr>
<td>Min RTT of Acct Req/Res</td>
<td>The minimum RTT of accounting access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Avg RTT of Acct Req/Res</td>
<td>The average RTT of accounting access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Max RTT of Acct Req/Res</td>
<td>The maximum RTT of accounting access requests or responses for the last seven days.</td>
</tr>
<tr>
<td>Last RTT of Acct Req/Res</td>
<td>Displays the last RTT of accounting access requests or responses.</td>
</tr>
<tr>
<td>BYOD</td>
<td>Displays the BYOD statistics.</td>
</tr>
<tr>
<td>Total No of COA Request</td>
<td>The total number of Change of Authorization (CoA) requests received from the server.</td>
</tr>
<tr>
<td>Total No of COA ACK Sent</td>
<td>The total number of CoA-ACKs sent to the server.</td>
</tr>
<tr>
<td>Total No of COA NACK Sent</td>
<td>The total number of CoA-NACKs sent to the server.</td>
</tr>
<tr>
<td>Total No of DM Request</td>
<td>The total number of disconnect request messages received from the server.</td>
</tr>
<tr>
<td>Total No of DM ACK Sent</td>
<td>Displays the total number of disconnect ACKs sent to the server.</td>
</tr>
<tr>
<td>Total No of DM NACK Sent</td>
<td>Displays the total number of disconnect NACKs sent to the server.</td>
</tr>
<tr>
<td>Time of last statistics clear</td>
<td>The date and time the AAA statistics were last cleared for the server.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.5R4; command was introduced.

### Related Commands

- **aaa radius-server**
  - Configures or modifies a RADIUS server for Authenticated Switch Access.
- **aaa radius-server health-check**
  - Enables or disables a RADIUS server health check.
- **aaa radius-server clear-statistics**
  - Clears statistics collected for the specified RADIUS server.
### MIB Objects

aaaAuthorServerStatsTable
- aaaAuthorStatsAccessReq
- aaaAuthorStatsAccessRes
- aaaAuthorStatsTimedOutReq
- aaaAuthorStatsCountRtt
- aaaAuthorStatsSumRtt
- aaaAuthorStatsMinRtt
- aaaAuthorStatsMaxRtt
- aaaAuthorStatsAvgRtt
- aaaAuthorStatsLastRtt

aaaAuthServerStatsTable
- aaaAuthStatsAccessReq
- aaaAuthStatsAccessRes
- aaaAuthStatsAccessAccept
- aaaAuthStatsAccessReject
- aaaAuthStatsAccessChal
- aaaAuthStatsTimedOutReq
- aaaAuthStatsCountRtt
- aaaAuthStatsSumRtt
- aaaAuthStatsMinRtt
- aaaAuthStatsMaxRtt
- aaaAuthStatsAvgRtt
- aaaAuthStatsLastRtt

aaaAcctServerStatsTable
- aaaAcctStatsAccessReq
- aaaAcctStatsAccessRes
- aaaAcctStatsTimedOutReq
- aaaAcctStatsCountRtt
- aaaAcctStatsSumRtt
- aaaAcctStatsMinRtt
- aaaAcctStatsMaxRtt
- aaaAcctStatsAvgRtt
- aaaAcctStatsLastRtt

aaaByodServerStatsTable
- aaaByodStatsCoaReq
- aaaByodStatsCoaAck
- aaaByodStatsCoaNack
- aaaByodStatsDmReq
- aaaByodStatsDmAck
- aaaByodStatsDmNack
aaa radius-server clear-statistics

Clears the AAA statistics collected for the specified RADIUS server.

aaa radius-server server_name clear-statistics

### Syntax Definitions

**server_name**

The name of the RADIUS server on which the AAA statistics will be cleared.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 \ V72/C32</th>
<th>6900 \ X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `show aaa server statistics` command to display the statistics collected for the specified server.

### Examples

- `-> aaa radius-server rad1 clear-statistics`
- `-> aaa radius-server rad2 clear-statistics`

### Release History

Release 8.5R4; command introduced.

### Related Commands

- **aaa radius-server** Configures or modifies a RADIUS server for Authenticated Switch Access and device authentication.
- **aaa radius-server health-check** Enables or disables a RADIUS server health check with the specified parameters.
- **show aaa server statistics** Displays authorization, authentication, accounting, and BYOD statistics collected for a RADIUS server.
MIB Objects

aaaServerTable
   aaasHostName
   aaasClearStats
show aaa authentication

Displays information about the current authenticated switch session.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `show aaa authentication` command to display authentication information about switch management services (Telnet, FTP, console port, Secure Shell, etc.).

Examples

-> show aaa authentication
Service type = Default
  1rst authentication server = RadiusServer
  2nd authentication server = local
Service type = Console
  1rst authentication server = local
Service type = Telnet
  Authentication = Use Default,
  1rst authentication server = RadiusServer
  2nd authentication server = local
Service type = FTP
  Authentication = Use Default,
  1rst authentication server = RadiusServer
  2nd authentication server = local
Service type = Http
  Authentication = Use Default,
  1rst authentication server = RadiusServer
  2nd authentication server = local
Service type = Snmp
  Authentication = Use Default,
  1rst authentication server = RadiusServer
  2nd authentication server = local
Service type = Ssh
  Authentication = Use Default,
  1rst authentication server  = TacacsServer
  2nd authentication server  = local

output definitions

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Displays denied if the management interface is disabled. Displays Use Default if the management interface is configured to use the default configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st authentication server</td>
<td>The first server to be polled for authentication information.</td>
</tr>
<tr>
<td>2nd authentication server</td>
<td>The next server to be polled for authentication information.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

**aaa authentication**  Configures the interface for Authenticated Switch Access and specifies the server(s) to be used.

MIB Objects

**aaaAuthSATable**
  aaatsName1
  aaatsName2
  aaatsName3
  aaatsName4
show aaa device-authentication

Displays a list of RADIUS servers assigned to provide 802.1X, MAC, or Captive Portal authentication.

`show aaa device-authentication [802.1x | mac | captive-portal]`

**Syntax Definitions**

- **802.1x** Displays the servers used for 802.1X authentication.
- **mac** Displays the servers used for MAC authentication.
- **captive-portal** Uses the servers used for Captive Portal authentication.

**Defaults**

By default, all assigned servers are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the optional **802.1x**, **mac**, or **captive-portal** parameters to display the servers assigned to provide the specified type of authentication.

**Examples**

```shell
-> show aaa device-authentication
Authentication type = mac
Authentication Server:
  1st authentication server = cppm,
  2nd authentication server = rad1
  3rd authentication server = rad2,
  4th authentication server = rad3

Authentication type = 802.1x
Authentication Server:
  1st authentication server = cppm,
  2nd authentication server = rad1

Authentication type = captive-portal
Authentication Server:
  1st authentication server = cppm,
  2nd authentication server = rad1
```
AAA Commands

show aaa device-authentication

## Output Definitions

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>The type of authentication the server is assigned to provide (802.1x, mac, or captive-portal)</td>
</tr>
<tr>
<td>1st authentication server</td>
<td>The first server to be polled for authentication information. Any backup servers are also displayed on subsequent lines.</td>
</tr>
</tbody>
</table>

## Release History

Release 7.2.1; command was introduced.
Release 7.3.4; 802.1x and mac parameters added.
Release 8.1.1; captive-portal parameter added.

## Related Commands

- **aaa device-authentication**  
  Configures the RADIUS server to use for 802.1X or MAC authentication.

## MIB Objects

- **AaaAuthMACTable**
  - aaaDaName1
  - aaaDaName2
  - aaaDaName3
  - aaaDaName4

---

**show aaa accounting**

Displays information about accounting servers configured for authenticated switch access and device authentication sessions. Accounting servers keep track of network resources (time, packets, bytes, etc.) and user activity.

**show aaa accounting [802.1x | mac | captive-portal]**

---

**Syntax Definitions**

- **802.1x**: Displays the RADIUS or syslog server used to log accounting for 802.1X authenticated sessions.
- **mac**: Displays the RADIUS or syslog server used to log accounting for MAC authenticated sessions.
- **captive-portal**: Displays the RADIUS or syslog server to log accounting for Captive Portal authenticated sessions.

**Defaults**

By default, the accounting server configuration is displayed for TACACS+ commands and management sessions (Telnet, FTP, console port, HTTP, or SNMP).

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **802.1x**, **mac**, or **captive-portal** parameters to display the accounting server configuration for a specific type of device authentication.
- If no parameters are entered with this command, the accounting server configuration for authentication sessions and TACACS+ commands is displayed.

**Examples**

```bash
-> show aaa accounting mac
Accounting type = mac
    Accounting Server:
        1st Acctnt Server = rad1,
        2nd Acctnt Server = rad2

-> show aaa accounting 802.1x
Accounting type = 802.1x
    Syslog Acctnt Server:
```

---
AAA Commands show aaa accounting

IP Address = 135.254.163.110,
UDP port = 514

-> show aaa accounting captive-portal
Accounting type = captive-portal
Syslog Acnt Server:
  IP Address = 135.254.163.110,
  UDP port = 514

-> show aaa accounting
Session (telnet, ftp, ...)
  1st accounting server = rad1
Command accounting server
  1st accounting server = server1

Release History

Release 7.1.1; command was introduced.
Release 8.1.1; 802.1x, mac, and captive-portal parameters added.

Related Commands

aaa accounting session
Configures an accounting server for authenticated switch access sessions.

aaa accounting command
Enables or disables the TACACS+ server for command accounting

aaa accounting
Configures RADIUS server accounting or local Switch Logging (syslog) accounting for device authentication sessions.

MIB Objects

aaaAcctDATable
  aaacdInterface
  aaacdName1
  aaacdName2
  aaacdName3
  aaacdName4
  aaacdSyslogIPAddrType
  aaacdSyslogIPAddr
  aaacdSyslogUdpPort
  aaacdRowStatus
show aaa config

Displays the AAA parameter configuration for 802.1X, MAC, and Captive Portal sessions.

show aaa \{802.1x | mac | captive-portal\} config

Syntax Definitions

802.1x Displays the parameter configuration for 802.1X authenticated sessions.
mac Displays the parameter configuration for MAC authenticated sessions.
captive-portal Displays the parameter configuration for Captive Portal authenticated sessions.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the 802.1x, mac, or captive-portal parameters to display the parameter configuration for a specific type of device authentication.

Examples

-> show aaa 802.1x config
Authentication type = 802.1x
Re-Authentication Timeout:
  Status = enable,
  Interval (sec) = 3600,
  Trust Radius = disable

Accounting Interim:
  Interval (sec) = 600,
  Trust Radius = disable

-> show aaa mac config
Authentication type = mac
Session Timeout:
  Status = disable,
  Interval (sec) = 43200,
  Trust Radius = disable
Inactivity Timeout:
  Status = disable,
  Interval (sec) = 600
Accounting Interim:
  Interval (sec) = 600,
  Trust Radius = disable

-> show aaa captive-portal config
Authentication type = captive-portal
Session Timeout:
  Status = disable,
  Interval (sec) = 43200,
  Trust Radius = disable
Inactivity Timeout:
  Status = disable,
  Interval (sec) = 600
Accounting Interim:
  Interval (sec) = 600,
  Trust Radius = disable

output definitions

<table>
<thead>
<tr>
<th>Authentication type</th>
<th>The type of authentication (802.1x, mac, or captive-portal).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Timeout</td>
<td>The parameter values for the AAA session timeout parameter. Does not apply to 802.1X authentication. Configured through the <code>aaa session-timeout</code> command.</td>
</tr>
<tr>
<td>Inactivity Logout</td>
<td>The parameter values for the AAA inactivity logout parameter. Does not apply to 802.1X authentication. Configured through the <code>aaa inactivity-logout</code> command.</td>
</tr>
<tr>
<td>Accounting Interim</td>
<td>The parameter values for the AAA accounting interim parameter. Configured through the <code>aaa interim-interval</code> command.</td>
</tr>
<tr>
<td>Re-authentication Timeout</td>
<td>The parameter values for the AAA 802.1X re-authentication timeout parameter. Does not apply to MAC or Captive Portal authentication. Configured through the <code>aaa 802.1x re-authentication</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.

Related Commands

- `show aaa device-authentication` Displays the device authentication server configuration.
- `show aaa accounting` Displays the accounting server configuration.
- `show aaa profile` Displays the AAA parameter profile configuration.
**MIB Objects**

alaAaaAuthConfig
alaAaa8021XReAuthStatus
alaAaa8021XReAuthIntrvl
alaAaa8021XReAuthTrustRadStatus
alaAaa8021XIntrmIntrvl
alaAaa8021XIntrmIntrvlTrstRadStus
alaAaaMacIntrmIntrvl
alaAaaMacIntrmIntrvlTrstRadStatus
alaAaaMacSessTimeoutStatus
alaAaaMacSessTimeoutIntrvl
alaAaaMacSessTimeoutTrstRadStatus
alaAaaMacInActLogoutStatus
alaAaaMacInActLogoutIntrvl
alaAaaCpIntrmIntrvl
alaAaaCpIntrmIntrvlTrstRadStatus
alaAaaCpSessTimeoutStatus
alaAaaCpSessTimeoutIntrvl
alaAaaCpSsTmotTrstRadStatus
alaAaaCpInActLogoutStatus
alaAaaCpInActLogoutIntrvl
show aaa radius config

Displays the global AAA attribute values and MAC address format.

show aaa radius config

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The MAC address format determines the delimiter character used between MAC address octets and whether or not characters are in uppercase or lowercase. This format is applied only when the RADIUS attribute value is set to a MAC address.

Examples

-> show aaa radius config
RADIUS client attributes:
  NAS port id             = default,
  NAS identifier          = default
  NAS IP address          = default
  MAC format delimiter:
    Username                = none, UsernameCase = uppercase,
    Password                = none, PasswordCase = uppercase,
    calling station id      = none, ClgStaIdCase = uppercase,
    called station id       = none, CldStaIdCase = uppercase
  Unp Profile Precedence  = Filter-Id

output definitions

NAS port id The RADIUS client NAS-Port attribute for authentication and accounting sessions.

NAS identifier The RADIUS client NAS-Identifier attribute for authentication and accounting sessions.
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAS IP address</td>
<td>The RADIUS client NAS-IP address attribute for authentication and accounting sessions.</td>
</tr>
<tr>
<td>MAC format delimiter</td>
<td>The MAC address format used in the specified RADIUS client attributes.</td>
</tr>
<tr>
<td>UNP Profile Precedence</td>
<td>The UNP profile precedence: Filter-ID or Tunnel-Private-Group-ID</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.
Release 8.5R4; UNP Profile Precedence and NAS IP address field added.

Related Commands

- **show aaa device-authentication**: Displays the device authentication server configuration.
- **show aaa accounting**: Displays the accounting server configuration.
- **show aaa profile**: Displays the AAA parameter profile configuration.
- **aaa radius nas-ip-address**: Configure the RADIUS client NAS IP address attribute for the outgoing RADIUS packets.

MIB Objects

```plaintext
alaAaaAuthConfig
    alaAaa8021XReAuthStatus
    alaAaa8021XReAuthIntrvl
    alaAaa8021XReAuthTrustRadStatus
    alaAaa8021XIntrvlIntrvl
    alaAaa8021XIntmIntrvlTrstRadStus
    alaAaaMacIntrvlIntrvl
    alaAaaMacIntmIntrvlTrstRadStatus
    alaAaaMacSessTimeoutStatus
    alaAaaMacSessTimeoutIntrvl
    alaAaaMacSessTimeoutTrstRadStus
    alaAaaMacInActLogoutStatus
    alaAaaMacInActLogoutIntrvl
    alaAaaCpIntrvlIntrvl
    alaAaaCpIntmIntrvlTrstRadStatus
    alaAaaCpSessTimeoutStatus
    alaAaaCpSessTimeoutIntrvl
    alaAaaCpSessTimeoutTrstRadStatus
    alaAaaCpInActLogoutStatus
    alaAaaCpInActLogoutIntrvl
```
### show aaa radius health-check-config

Displays the RADIUS server health check configuration for each RADIUS server.

#### Syntax Definitions

**N/A**

#### Defaults

**N/A**

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

This command displays the health check configuration for all RADIUS servers defined on the switch.

#### Examples

```
-> show aaa radius health-check-config
Server Name  Health Check  Polling Interval  Failover Status  Username
RAD1          DISABLED     60             DISABLED        alcatel
RAD2          ENABLED      90             ENABLED         alcatel
```

#### Output Definitions

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>The name of the RADIUS server.</td>
</tr>
<tr>
<td>Health Check</td>
<td>The operational status of the RADIUS health check feature for the server.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>The configured polling interval for the RADIUS server.</td>
</tr>
<tr>
<td>Failover Status</td>
<td>The status of the failover operation. When enabled, the re-authentication of users assigned to the authentication server down profile is triggered when the RADIUS server comes back up before the authentication server down timeout value expires).</td>
</tr>
<tr>
<td>Username</td>
<td>The configured user name for RADIUS server polling.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

`aaa radius-server health-check`  
Configures RADIUS health check for the specified RADIUS server.

**MIB Objects**

`aaaServerTable`  
`aaasHostName`  
`aaasRadHealthCheck`  
`aaasRadPollingInterval`  
`aaasRadFailover`  
`aaasRadUsername`
show aaa profile

Displays the AAA profile configuration.

show aaa profile [profile_name]

---

Syntax Definitions

profile_name

The name of an existing AAA profile.

---

Defaults

By default, all profiles are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enter an AAA profile name with this command to display information about a specific profile.

Examples

-> show aaa profile ap2

AAA profile name = ap2
Authentication type = mac
  Authentication Server:
    1st Auth Server = rad1,
    2nd Auth Server = rad2

Accounting Server:
  1st Accnt Server = rad1,
  2nd Accnt Server = rad2

Session Timeout:
  Status = disable,
  Interval (sec) = 43200,
  Trust Radius = disable

Inactivity Timeout:
  Status = disable,
  Interval (sec) = 600

Accounting Interim:
  Interval (sec) = 600,
AAA Commands

show aaa profile

Trust Radius = disable
Authentication type = 802.1x
Re-Authentication Timeout:
  Status = disable,
  Interval (sec) = 3600,
  Trust Radius = disable

Accounting Interim:
  Interval (sec) = 600,
  Trust Radius = disable

Authentication type = captive-portal
Session Timeout:
  Status = disable,
  Interval (sec) = 43200,
  Trust Radius = disable

Inactivity Timeout:
  Status = disable,
  Interval (sec) = 600

Accounting Interim:
  Interval (sec) = 600,
  Trust Radius = disable

RADIUS client attributes:
  NAS port id = default,
  NAS identifier = default,
  NAS ip address = default,
  MAC format delimiter:
    Username = none, UserNameCase = uppercase,
    Password = none, PasswordCase = uppercase,
    calling station id = none, ClgStaIdCase = uppercase,
    called station id = none, CldStaIdCase = uppercase

output definitions

<table>
<thead>
<tr>
<th>Authentication type</th>
<th>The type of authentication (802.1x, mac, or captive-portal) configured through the profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Timeout</td>
<td>The profile values defined for the AAA session timeout parameter. Does not apply to 802.1X authentication.</td>
</tr>
<tr>
<td>Inactivity Logout</td>
<td>The profile values defined for the AAA inactivity logout parameter. Does not apply to 802.1X authentication.</td>
</tr>
<tr>
<td>Accounting Interim</td>
<td>The profile values defined for the AAA accounting interim parameter.</td>
</tr>
<tr>
<td>Re-authentication Timeout</td>
<td>The profile values defined for the AAA re-authentication timeout parameter. Does not apply to MAC or Captive Portal authentication.</td>
</tr>
<tr>
<td>RADIUS client attributes</td>
<td>The profile values defined for the NAS-Port, NAS-Port-Identifier and the NAS-IP address attributes and the format to use when the specified attribute value is set to a MAC address.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.
Release 8.5R4; NAS IP address output field added.
Related Commands

**aaa profile**

Configures an AAA profile.

MIB Objects

alaAaaProfTable

alaAaaProfOnexReAuthSts
alaAaaProfOnexReAuthIntrvl
alaAaaProfOnexReAuthTrstRadSts
alaAaaProfOnexIntmIntrvl
alaAaaProfOnexIntmItvlTstRadSts
alaAaaProfMacIntmIntrvl
alaAaaProfMacIntmItvlTstRadSts
alaAaaProfMacSessTimeoutSts
alaAaaProfMacSessTimeoutIntrvl
alaAaaProfMacSessTmoutTrstRadSts
alaAaaProfMacInActLogoutSts
alaAaaProfMacInActLogoutIntrvl
alaAaaProfCpSessTimeoutSts
alaAaaProfCpSessTimeoutIntrvl
alaAaaProfCpSessTmoutTrstRadSts
alaAaaProfCpInActLogoutSts
alaAaaProfCpInActLogoutIntrvl
alaAaaProfCpIntrmIntrvl
alaAaaProfCpIntrmTrstRadSts
alaAaaProfRadNasPortId
alaAaaProfRadNasIdentifier
alaAaaProfRadUsernameDelim
alaAaaProfRadPasswordDelim
alaAaaProfRadCallInStnIdDelim
alaAaaProfRadCallOutStnIdDelim
alaAaaProfRadUsernameCase
alaAaaProfRadPasswordCase
alaAaaProfRadCallInStnIdCase
alaAaaProfRadCallOutStnIdCase
show aaa session console config

Displays the current administrative state of the session console configuration.
show aaa session console config

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples
-> show aaa session console config
Console access admin-state: disabled

Release History
Release 8.6R2; command introduced.

Related Commands
aaa session console Enables or disables switch access through the console port of the switch

MIB Objects
N/A
show user

Displays information about all users or a particular user configured in the local user database on the switch.

show user [username]

Syntax Definitions

username The name of the user. Used for logging into the switch.

Defaults

By default, all users are displayed if the username parameter is not specified with this command.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to display information about read/write access and partitioned management access (domains and families).

Examples

-> show user
User name = Customer1,
Password expiration = 10/27/2010 11:01 (30 days from now),
Password allow to be modified date = 9/30/2010 10:59 (3 days from now),
Account lockout = Yes (Automatically unlocked after 19 minute(s) from now),
Password bad attempts = 3,
Read Only for domains = None,
Read/Write for domains = Admin System Physical Layer2 Services policy Security,
Read/Write for families = ip rip ospf bgp vrrp ip-routing ipx ipmr ipms,
Snp allowed = YES,
Snp authentication = SHA,
Snp encryption = DES,
Console-Only = Disabled,
SSH allowed = NO,
User name = admin,
Password expiration = 10/27/2010 11:01 (30 days from now),
Password allow to be modified date = 9/30/2010 10:59 (3 days from now),
Account lockout = None,
Password bad attempts = 0,
Read Only for domains = None,
Read/Write for domains = All,
Snp allowed = NO,
Console-Only = Disabled,
SSH allowed = NO,
output definitions

<table>
<thead>
<tr>
<th>User name</th>
<th>The user name for this account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password expiration</td>
<td>The date and time on which the password will expire. This field only displays if the password expiration is configured specifically for a user, or a default password expiration is configured globally on the switch through the user password-expiration command. (Note that the date/time are based on the switch’s default system date/time or the system date/time configured through the system date and system time commands.)</td>
</tr>
<tr>
<td>Password allow to be modified date</td>
<td>The earliest date and time on which the user may change the password. Configured through the user password-min-age command.</td>
</tr>
<tr>
<td>Account lockout</td>
<td>Indicates if the user account is locked out (Yes or No) and how many minutes remain until the user account is automatically unlocked. If no remaining time is displayed, the admin user or a user with admin privileges must manually unlock the account. Configured through the user lockout-duration and user lockout unlock commands.</td>
</tr>
<tr>
<td>Password bad attempts</td>
<td>The number of failed password login attempts for this user account.</td>
</tr>
</tbody>
</table>

Read Only for domains

The command domains available with the user’s read-only access. See the table on the next page for a listing of valid domains.

Read/Write for domains

The command domains available with the user’s read-write access. See the table on the next page for a listing of valid domains.

Read Only for families

The command families available with the user’s read-only access. See the table on the next page for a listing of valid families.

Read/Write for families

The command families available with the user’s read-write access. See the table on the next page for a listing of valid families.

Snmp allowed

Indicates whether or not the user is authorized to use SNMP (YES or NO). SNMP is allowed for the user account when SNMP authentication is specified for the account.

Snmp authentication

The level of SNMP authentication, if any, configured for the user. This field only displays if the user is authorized to use SNMP.

Snmp encryption

The level of SNMP encryption, if any, configured for the user. This field only displays if the user is authorized to use SNMP.

Console-Only

Indicates whether or not console only access is enabled or disabled for the user admin.

SSH allowed

Indicates whether or not SSH access to the switch is enabled or disabled for a specific user.

Possible values for command domains and families are listed here:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Corresponding Families</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-admin</td>
<td>file telnet dshell debug</td>
</tr>
<tr>
<td>domain-system</td>
<td>system aip snmp rmon webmgt config</td>
</tr>
<tr>
<td>domain-physical</td>
<td>chassis module interface pmm health</td>
</tr>
<tr>
<td>domain-network</td>
<td>ip rip ospf bgp vrrp ip-routing ipx ipmr ipms</td>
</tr>
<tr>
<td>domain-layer2</td>
<td>vlan bridge stp 802.1q linkagg ip-helper</td>
</tr>
</tbody>
</table>
AAA Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-service</td>
<td>DNS configuration options</td>
</tr>
<tr>
<td>domain-policy</td>
<td>Quality of Service policies for load balancing</td>
</tr>
<tr>
<td>domain-security</td>
<td>Session Layer 4 policies for access control</td>
</tr>
<tr>
<td>user</td>
<td>Configures user entries in the local user database.</td>
</tr>
<tr>
<td>show user password-policy</td>
<td>Displays the global password policy configuration for the switch.</td>
</tr>
<tr>
<td>show user lockout-setting</td>
<td>Displays the global user lockout settings for the switch.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Release 8.8R2; **SSH allowed** field added.

**Related Commands**

- **user**
  - Configures user entries in the local user database.
- **show user password-policy**
  - Displays the global password policy configuration for the switch.
- **show user lockout-setting**
  - Displays the global user lockout settings for the switch.

**MIB Objects**

aaaUserTable
  - aaaUserName
  - aaaPasswordExpirationDate
  - aaaPasswordExpirationInMinute
  - aaaPasswordAllowModifyDate
  - aaaPasswordLockoutEnable
  - aaaBadAttempts
  - aaaReadRight1
  - aaaReadRight2
  - aaaWriteRight1
  - aaaWriteRight2
  - aaaSnmpLevel
  - aaaSnmpAuthkey
show user password-policy

Displays the global password settings configured for the switch.

show user password-policy

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The password policy contains parameter values that define configuration requirements for all passwords that are created on the switch. Use this command to display the current parameter values for the password policy.

Examples

-> show user password-policy
Password Policy:
Password cannot contain username: Yes
Minimum number of English uppercase characters: 6
Minimum number of English lowercase characters: 4
Minimum number of base-10 digit: 2
Minimum number of non-alphanumeric: 3
Minimum size : 8
Password history: 4
Password minimum age: 20 (days)
Password expiration: 100 (days)
**output definitions**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password cannot contain username</td>
<td>Indicates if the username is included with the password check (Enable or Disable). Configured through the <code>user password-policy cannot-contain-username</code> command.</td>
</tr>
<tr>
<td>Minimum number of English uppercase characters</td>
<td>The minimum number of uppercase characters required in a password. Configured through the <code>user password-policy cannot-contain-consecutive-characters</code> command.</td>
</tr>
<tr>
<td>Minimum number of English lowercase characters</td>
<td>The minimum number of lowercase characters required in a password. Configured through the <code>user password-policy min-lowercase</code> command.</td>
</tr>
<tr>
<td>Minimum number of base-10 digit</td>
<td>The minimum number of digits required in a password. Configured through the <code>user password-policy min-digit</code> command.</td>
</tr>
<tr>
<td>Minimum number of non-alphanumeric</td>
<td>The minimum number of non-alphanumeric characters required in a password. Configured through the <code>user password-policy min-nonalpha</code> command.</td>
</tr>
<tr>
<td>Minimum size</td>
<td>The minimum number of characters required for the password size. Configured through the <code>super-password</code> command.</td>
</tr>
<tr>
<td>Password history</td>
<td>The maximum number of old passwords retained in the password history. Configured through the <code>user password-history</code> command.</td>
</tr>
<tr>
<td>Password minimum age</td>
<td>The number of days a password is protected from any modification. Configured through the <code>user password-min-age</code> command.</td>
</tr>
<tr>
<td>Password expiration</td>
<td>The default expiration date applied to all passwords. Configured through the <code>user password-expiration</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show user password-policy` Displays the expiration date for passwords configured for user accounts stored on the switch.

**MIB Objects**

`aaaAsaConfig`

- `aaaAsaPasswordMinUpperCase`
- `aaaAsaPasswordMinLowerCase`
- `aaaAsaPasswordMinDigit`
- `aaaAsaPasswordMinNonAlpha`
- `aaaAsaPasswordHistory`
- `aaaAsaPasswordMinAge`
- `aaaAsaPasswordSizeMin`
- `aaaAsaDefaultPasswordExpirationInDays`
show user lockout-setting

Displays the global user lockout settings for the switch.

show user lockout-setting

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The global lockout settings include parameter values that determine the length of a user observation window, the amount of time a locked user remains locked, and the number of failed password login attempts allowed.

Examples

-> show user lockout-setting
Lockout Setting:
Observation window: 30 (minutes)
Duration: 200 (minutes)
Threshold: 20

output definitions

<table>
<thead>
<tr>
<th>Observation window</th>
<th>The amount of time, in minutes, during which the number of failed password login attempts are counted. Configured through the user lockout-window command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>The amount of time, in minutes, that a locked user account remains locked out of the switch. Configured through the user lockout-duration command.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The maximum number of failed password login attempts allowed before the user is locked out of the switch. Configured through the user lockout-threshold command.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **user lockout unlock**
  Manually locks or unlocks a user account on the switch.

- **show user**
  Displays information about all users or a particular user configured in the local user database on the switch.

**MIB Objects**

- **aaaAsaConfig**
  - **aaaAsaLockoutWindow**
  - **aaaAsaLockoutDuration**
  - **aaaAsaLockoutThreshold**
show aaa priv hexa

Displays hexadecimal values for command domains/families. Useful for determining how to express command families in hexadecimal; hexadecimal values are used in configuring user privileges in attributes on an external LDAP or RADIUS authentication server.

show aaa priv hexa [domain or family]

Syntax Definitions

domain or family

The CLI command domain or particular command family for which you want to display hexadecimal values. See table in Usage Guidelines.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Corresponding Families</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-admin</td>
<td>file telnet dshell debug</td>
</tr>
<tr>
<td>domain-system</td>
<td>system aip snmp rmon webmgmt config</td>
</tr>
<tr>
<td>domain-physical</td>
<td>chassis module interface pmm health</td>
</tr>
<tr>
<td>domain-network</td>
<td>ip rip ospf bgp vrrp ip-routing ipx ipmr ipms</td>
</tr>
<tr>
<td>domain-layer2</td>
<td>vlan bridge stp 802.1q linkagg ip-helper</td>
</tr>
<tr>
<td>domain-service</td>
<td>dns</td>
</tr>
<tr>
<td>domain-policy</td>
<td>qos policy slb</td>
</tr>
<tr>
<td>domain-security</td>
<td>session avlan aaa</td>
</tr>
</tbody>
</table>

- Valid values for the family parameter are listed in the Corresponding Families column of the following table:

- Note that some command families may not be supported depending on the hardware platform you are running.
- If you do not specify a command family, hexadecimal values for all commands sets will display.
- The ‘lanpower’ commands were moved from the ‘module’ family to the ‘lanpower’ family in 8.8R1.
Examples

-> show aaa priv hexa

- file = 0x00000001 0x00000000,
- telnet = 0x00000008 0x00000000,
- dshell = 0x00000020 0x00000000,
- debug = 0x00000040 0x00000000,
- domain-admin = 0x00000069 0x00000000,
- system = 0x00000080 0x00000000,
- aip = 0x00000100 0x00000000,
- snmp = 0x00000200 0x00000000,
- rmon = 0x00000400 0x00000000,
- webmgt = 0x00000800 0x00000000,
- config = 0x00001000 0x00000000,
- domain-system = 0x00001F80 0x00000000,
- chassis = 0x00002000 0x00000000,
- module = 0x00004000 0x00000000,
- interface = 0x00008000 0x00000000,
- pmm = 0x00010000 0x00000000,
- health = 0x00040000 0x00000000,
- domain-physical = 0x0005E000 0x00000000,
- ip = 0x00080000 0x00000000,
- rip = 0x00100000 0x00000000,
- ospf = 0x00200000 0x00000000,
- bgp = 0x00400000 0x00000000,
- vrrp = 0x00800000 0x00000000,
- ip-routing = 0x01000000 0x00000000,
- ipx = 0x02000000 0x00000000,
- ipmr = 0x04000000 0x00000000,
- ipms = 0x08000000 0x00000000,
- domain-network = 0x00FF8000 0x00000000,
- vlan = 0x10000000 0x00000000,
- bridge = 0x20000000 0x00000000,
- stp = 0x40000000 0x00000000,
- 802.1q = 0x80000000 0x00000000,
- linkagg = 0x00000000 0x00000001,
- ip-helper = 0x00000000 0x00000002,
- domain-layer2 = 0xF0000000 0x00000003,
- dns = 0x00000000 0x00000010,
- domain-service = 0x00000000 0x00000010,
- qos = 0x00000000 0x00000020,
- policy = 0x00000000 0x00000040,
- sla = 0x00000000 0x00000080,
- domain-policy = 0x00000000 0x000000E0,
- session = 0x00000000 0x00000010,
- avlan = 0x00000000 0x00000040,
- aaa = 0x00000000 0x00000080,
- domain-security = 0x00000000 0x000000D0

-> show aaa priv hexa rip

0x00100000 0x00000000
Release History
Release 7.1.1; command was introduced.

Related Commands
user Configures or modifies user entries in the local user database.

MIB Objects
N/A
**show system fips**

Displays the administrative and operational status of the FIPS mode on the switch.

```bash
show system fips
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `show system fips` command is the only command that can be used to view the FIPS mode status. The FIPS status is not shown in the `show configuration snapshot` command output.

### Examples

```bash
-> show system fips
Admin State: Enabled
Oper State: Enabled
```

### Release History

Release 8.1.1; command introduced.

### Related Commands

- `aaa authentication`  
  Enable or disable the FIPS mode on the switch.

### MIB Objects

- `systemFipsAdminState`
- `systemFipsOperState`
aaa switch-access mode

Globally sets the access mode as enhanced or default.

aaa switch-access mode {default | enhanced}

**Syntax Definitions**

default
Sets the access mode as default.

enhanced
Sets the access mode as enhanced.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>default</td>
</tr>
<tr>
<td>enhanced</td>
<td>default</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

It is recommended to save configuration and reboot the switch when the ASA access mode is configured.

**Example**

-> aaa switch-access mode default

-> aaa switch-access mode enhanced

WARNING: Recommended to save configuration and reload the switch upon switch access mode change.

**Release History**

Release 8.3.1; command introduced.
Related Commands

show aaa switch-access mode  Displays the access mode configuration.

MIB Objects

aaaAsaConfig
  aaaAsaAccessMode
aaa switch-access ip-lockout-threshold

Configures the threshold value for failed login attempts from an IP address after which the IP address will be banned from switch access.

aaa switch-access ip-lockout-threshold number

Syntax Definitions

number Set the threshold value for login attempts in the range 0 to 999.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>6</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The command is applicable only if ASA enhanced mode is enabled.
- Set the IP threshold value to ‘0’ to disable the IP lockout thresholds.
- IP address is permanently blocked/banned if the number of authentication failures from a particular IP reaches IP lockout threshold limit within two times of the user lockout window.
- Only the switch access will be restricted from the banned IP address. Any IP packet (with monitored port number) destined to a switch IP interfaces will be discarded. IP packets normally bridged/routed by the switch will not be discarded.
- A maximum of 128 IP addresses can be added to the banned list. When the maximum limit has reached, oldest entry from the list is removed to accommodate the new entries.
- User lockout window (user lockout-window) is applicable for IP lockout threshold as well.
- IP lockout threshold shall share the same window as user lockout window, and by default, IP lockout threshold shall be two times that of user lockout window. Since user lockout is giving more priority, the IP lockout threshold must be greater than the user lockout threshold value.
- The IP address will remain blocked until it is released using the command aaa switch-access banned-ip release.
**Example**

-> aaa switch-access ip-lockout-threshold 2

**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `aaa switch-access mode`  Globally sets the access mode as enhanced or default.
- `show aaa switch-access ip-lockout-threshold` Displays the lockout threshold configured for the remote IP addresses.

**MIB Objects**

- `aaaAsaConfig`  
  `aaaAsaAccessIpLockoutThreshold`
aaa switch-access banned-ip release

Releases the banned IP addresses that are blocked due to failed login attempts.

aaa switch-access banned-ip {all | ip_address} release

Syntax Definitions

- **all**: Release all banned IP addresses from the banned list.
- **ip_address**: Release a specific IP address from the banned list.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The IP addresses are banned if the failed login count reaches IP lockout threshold limit.

Example

- `-> aaa switch-access banned-ip all release`
- `-> aaa switch-access banned-ip 100.2.45.56 release`

Release History

Release 8.3.1; command introduced.

Related Commands

- `show aaa switch-access banned-ip`: Displays the list of banned IP addresses.

MIB Objects

- `aaaSwitchAccessBannedIpTable`
- `aaaSwitchAccessBannedIpAddress`
- `aaaSwitchAccessBannedIpRowStatus`
**aaa switch-access priv-mask**

Configure the functional privileges mask for the switch access based on the access type on top of the user privilege.

`aaa switch-access priv-mask {console | telnet | ssh | http | https} {read-only | read-write} [families... | domains... | all | none | all-except families...]`

### Syntax Definitions

**read-only**

Specifies that the user will have read-only access to the switch through a specific access type.

**read-write**

Specifies that the user will have read-write access to the switch through a specific access type. The read-write access is allowed only for http, https access types. For other access types (console, telnet, and ssh only) read-only access is allowed.

**families**

Determines the command families available to the user on the switch for a specific access type. Each command family should be separated by a space. Command families are subsets of domains. See Usage Guidelines for more details.

**domains**

Determines the command domains available to the user on the switch for a specific access type. Each domain should be separated by a space. See the Usage Guidelines for more details.

**all**

Specifies that all command families and domains are available to the user for a specific access type.

**none**

Specifies that no command families or domains are available to the user for a specific access type.

**all-except**

Specifies that functional privileges for families followed by 'all-except' are disabled for a specific access type.

### Defaults

By default, the access types are enabled with read-write privileges for all the families.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The command is applicable only when ASA enhanced mode is enabled.
- The access privileges for the SSH, TELNET, Console, HTTP, HTTPS can be defined.
AAA Commands

- The read-write privilege can be applied only for HTTP and HTTPS access types.
- For SSH, TELNET, and Console, only read-only privilege can be applied.
- Possible values for domains and families are listed in the following table:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Corresponding Families</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain-admin</td>
<td>file telnet debug</td>
</tr>
<tr>
<td>domain-system</td>
<td>system aip snmp rmon webmgt config</td>
</tr>
<tr>
<td>domain-physical</td>
<td>chassis module interface pmm health</td>
</tr>
<tr>
<td>domain-network</td>
<td>ip rip ospf bgp vrrp ip-routing ipmr ipms</td>
</tr>
<tr>
<td>domain-layer2</td>
<td>vlan bridge stp 802.1q linkagg ip-helper</td>
</tr>
<tr>
<td>domain-service</td>
<td>dns</td>
</tr>
<tr>
<td>domain-policy</td>
<td>qos policy slb</td>
</tr>
<tr>
<td>domain-security</td>
<td>session avlan aaa</td>
</tr>
<tr>
<td>domain-mpls</td>
<td>mpls</td>
</tr>
<tr>
<td>domain-datacenter</td>
<td>fips, auto-fabric</td>
</tr>
<tr>
<td>domain-afn</td>
<td>sip-snooping, dpi, app-mon</td>
</tr>
</tbody>
</table>

**Example**

- `aaa switch-access priv-mask ssh read-only webmgt vrrp vrf vlan udld`
- `aaa switch-access priv-mask telnet read-write tftp-client telnet system stp ssh`
- `aaa switch-access priv-mask ssh read-only all-except vlan`
- `aaa switch-access priv-mask telnet read-write all-except ip`

If privileges for specific families need to be applied, then remove the existing privilege using the `no` command, and re-apply the required family privilege.

- `no aaa switch-access priv-mask telnet read-write all`
- `aaa switch-access priv-mask telnet read-write vlan aaa`

**Release History**

Release 8.3.1; command introduced.
Related Commands

- **aaa switch-access mode**
  Globally sets the access mode as enhanced or default.

- **show aaa switch-access priv-mask**
  Displays the privilege details for the access types.

MIB Objects

- `aaaSwitchAccessPrivMaskTable`
- `aaaSwitchAccessType`
- `aaaSwitchAccessReadRight1`
- `aaaSwitchAccessReadRight2`
- `aaaSwitchAccessReadRight3`
- `aaaSwitchAccessReadRight4`
- `aaaSwitchAccessWriteRight1`
- `aaaSwitchAccessWriteRight2`
- `aaaSwitchAccessWriteRight3`
- `aaaSwitchAccessWriteRight4`
aaa switch-access management-stations admin-state

Enables or disables the IP management station feature in a switch.

aaa switch-access management-stations admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the IP management station feature in the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the IP management station feature in the switch.</td>
</tr>
</tbody>
</table>

Defaults

The IP management station feature is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The command is applicable only when ASA enhanced mode is enabled.
- When the IP management station is disabled, switch access from any IP address shall be allowed. If there is a login failure (based on the ip-lockout threshold value), the IP address will be banned/ blocked and added to the banned IP address list.
- When the IP management station is enabled, the switch access will be allowed only from those IPs configured in the management station list and only if those are not in banned list.
- It is recommended to enable this command from console since this may terminate the existing session, if enabled through telnet or SSH.

Example

- -> aaa switch-access management-stations admin-state enable
- -> aaa switch-access management-stations admin-state disable

Release History

Release 8.3.1; command introduced.
Related Commands

- **aaa switch-access mode**
  Globally sets the access mode as enhanced or default.

- **aaa switch-access management-stations**
  Configure the management station in the switch, with or without mask value for the corresponding IP of the management station.

- **show aaa switch-access management-stations**
  Displays the list of configured management stations.

MIB Objects

- **aaaSwitchAccessMgmtStationTable**
- **aaaSwitchAccessMgmtStationRowStatus**
aaa switch-access management-stations

Configure the management station in the switch, with or without mask value for the corresponding IP of the management station. The remote access is allowed only from these IP addresses if management station feature is enabled.

aaa switch-access management-stations [ip_address | ip_address /mask]

no aaa switch-access management-stations ip_address

Syntax Definitions

ip_address

IP address and the mask of the management station.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The command is configurable when `aaa switch-access management-stations admin-state` is enabled.
- A maximum of 64 management stations can be configured.
- Removing an IP address from the management station list will not remove the IP from the banned list.
- Whenever an IP address is removed from the management station, switch will stop responding to that IP. However, the existing sessions are not terminated automatically.

Example

`-> aaa switch-access management stations 100.15.9.8`
`-> aaa switch-access management stations 100.15.9.9 255.255.255.0`

Release History

Release 8.3.1; command introduced.
**Related Commands**

- `aaa switch-access management-stations admin-state`
  Enables or disables the IP management station feature in a switch.

- `show aaa switch-access management-stations`
  Displays the list of configured management stations.

**MIB Objects**

- `aaaSwitchAccessMgmtStationTable`
- `aaaSwitchAccessMgmtStationIpAddress`
show aaa switch-access mode

Displays the access mode configuration.

show aaa switch-access mode

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Example

-> show aaa switch-access mode
AAA Switch Access:
  Switch Access Mode = Default,
  Restricted Management Station = Disabled

output definitions

<table>
<thead>
<tr>
<th></th>
<th>ASA access mode: Enhanced or Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Access Mode</td>
<td></td>
</tr>
<tr>
<td>Restricted Management Station</td>
<td>The status of the IP management station feature in a switch: Enabled or Disabled</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command introduced.

Related Commands

aaa switch-access mode Globally sets the access mode as enhanced or default.

MIB Objects

aaaAsaConfig
AAA Commands

show aaa switch-access mode

aaaAsaAccessMode
show aaa switch-access ip-lockout-threshold

Displays the IP lockout threshold value.

show aaa switch-access ip-lockout-threshold

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900/V72/C32</th>
<th>6900/X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Example

-> show aaa switch-access ip-lockout-threshold
ip Lockout Threshold = 6

Output definitions

| IP lockout threshold | The IP lockout threshold value. |

Release History
Release 8.3.1; command introduced.

Related Commands

aaa switch-access ip-lockout-threshold

Configures the threshold for failed login attempts from an IP address after which the IP address will be banned from switch access.

MIB Objects

aaaAsaConfig

aaaAsaAccessIpLockoutThreshold
show aaa switch-access banned-ip

Displays the list of banned IP addresses.

show aaa switch-access banned-ip

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Example

-> show aaa switch-access banned-ip

<table>
<thead>
<tr>
<th>S. No</th>
<th>Banned IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100.15.5.21</td>
</tr>
<tr>
<td>2</td>
<td>100.15.5.22</td>
</tr>
</tbody>
</table>

output definitions

Banned IP address The banned IP address blocked due to failed login attempts.

Release History

Release 8.3.1; command introduced.
Related Commands

**aaa switch-access banned-ip release**  Releases the banned IP addresses that are blocked due to failed login attempts.

MIB Objects

```
aaaSwitchAccessBannedIpTable
   aaaSwitchAccessBannedIpAddress
```
show aaa switch-access priv-mask

Displays the privilege details for the access types.

show aaa switch-access priv-mask

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>9000</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show aaa switch-access priv-mask
Interface Type = CONSOLE,
    Read Only for domains = All ,
    Read/Write for domains = All
Interface Type = TELNET,
    Read Only for domains = All ,
    Read/Write for domains = All
Interface Type = SSH,
    Read Only for domains = All ,
    Read/Write for domains = All
Interface Type = HTTP,
    Read Only for domains = All ,
    Read/Write for domains = All
Interface Type = HTTPS,
    Read Only for domains = All ,
    Read/Write for domains = All

output definitions

<table>
<thead>
<tr>
<th>Interface Type</th>
<th>The interface type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Only for domains</td>
<td>Read-only privileges for the domains.</td>
</tr>
<tr>
<td>Read/Write for domains</td>
<td>Read-write privileges for the domains.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.3.1; command introduced.

**Related Commands**

`aaa switch-access priv-mask`  Configure the functional privileges for a particular access type.

**MIB Objects**

aaaSwitchAccessPrivMaskTable
  aaaSwitchAccessType
  aaaSwitchAccessReadRight1
  aaaSwitchAccessReadRight2
  aaaSwitchAccessReadRight3
  aaaSwitchAccessReadRight4
  aaaSwitchAccessWriteRight1
  aaaSwitchAccessWriteRight2
  aaaSwitchAccessWriteRight3
  aaaSwitchAccessWriteRight4
show aaa switch-access management-stations

Displays the list of configured management stations.

show aaa switch-access management-stations

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples
-> show aaa switch-access management-stations
AAA Switch Access:
Restricted Management station = ENABLED
  Management Subnet
  IP Address Prefix
-----------------------------
  100.15.5.21  255.255.255.255

output definitions

<table>
<thead>
<tr>
<th>Restricted Management station</th>
<th>IP management station status: Enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IP address</td>
<td>IP address of the management station.</td>
</tr>
<tr>
<td>Subnet Prefix</td>
<td>The prefix corresponding to the IP address.</td>
</tr>
</tbody>
</table>

Release History
Release 8.3.1; command introduced.
Related Commands

- **aaa switch-access management-stations admin-state**
  Enables or disables the IP management station feature in a switch.

- **aaa switch-access management-stations**
  Configure the management station in the switch, with or without mask value for the corresponding IP of the management station.

MIB Objects

- **aaaSwitchAccessMgmtStationTable**
  - **aaaSwitchAccessMgmtStationRowStatus**
  - **aaaSwitchAccessMgmtStationIpAddress**
show aaa switch-access hardware-self-test

Displays the major hardware component status.

show aaa switch-access hardware-self-test

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
The command is applicable only when ASA Enhanced mode is enabled.

Examples

Output for admin user
-> show aaa switch-access hardware-self-test
Checking CPU status -> Ok
Checking Memory status -> Ok
Checking Flash Status -> Ok
Checking NI Module status -> Ok
Checking Power Supply status -> Ok
Checking Lanpower Status -> Ok
Checking GBIC Status -> Ok

Output for secureadmin user
-> show aaa switch-access hardware-self-test
Checking CPU Status ---> Ok
CPU usage: ..............10% (Good: 0-30%, Warning: 30%-70%, Critical: 70% -)
CPU status: ..............running -> Ok
Checking Memory Status ---> OK
Memory usage: 100Mb
Memory status: Ok
Checking Flash Status ---> Ok
Flash usage: 980MB. -> Ok
Checking NI Module Status ---> NOk
NI#1 status: UP
NI#2 status: Down
NI#3 status: UP
Checking Power Supply Status ---> Ok
Power supply #1: Ok
Power supply #2: Ok

**Release History**

Release 8.3.1; command introduced.
Release 8.8R1; output updated for `secureadmin` user.

**Related Commands**

- show aaa switch-access process self-test

**MIB Objects**

- N/A
show aaa switch-access process-self-test

Displays the major software process status.

show aaa switch-access process-self-test

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The command is applicable only when ASA enhanced mode is enabled.

Examples

Output for admin user

--> show aaa switch-access process-self-test
-----------------------------------
    Process Self Test
-----------------------------------
    Checking Chassis Supervision Process -> Ok
    Checking AAA Process -> Ok
    Checking Configuration Manager Process -> Ok
    Checking Network Process -> Ok
    Checking QoS Process ---> Ok
    Checking VLAN Manager Process -> Ok
    Checking H/W Driver Process -> Ok
    Checking Layer2/Switching -> Ok
    Checking Layer3/Switching -> Ok

Output for secureadmin user

--> show aaa switch-access process-self-test
-----------------------------------------------
    Starting Process Self-Test
-----------------------------------------------
    cat proc new_cs stat ---> "Running"
    Chassis Supervision Process ---> Ok
AAA Commands

Checking AAA Process...
cat proc aaccommm stat  ---> "Running"
AAA Process ---> Ok
Checking Configuration Manager Process...
cat proc confd stat  ---> "Running"
Configuration Manager Process ---> Ok
Checking Network Process...
cat proc etherCmm stat  ---> "Running"
Network Process ---> Ok
Checking QoS Process...
cat proc qosCmmd stat  ---> "Running"
QoS Process ---> Ok
Checking VLAN Manager Process...
cat proc vmCmm stat  ---> "Running"
VLAN Manager Process ---> Ok
Checking Layer2/Switching Processes...
cat proc stpCmm stat  ---> "Running"
cat proc lagCmm stat  ---> "Running"
cat proc slCmm stat  ---> "Running"
cat proc lldpCmm stat  ---> "Running"
Layer2/Switching Processes ---> Ok
Checking Layer3/Switching Processes...
cat proc ip6cmmd stat  ---> "Running"
cat proc ipsec6d stat  ---> "Running"
cat proc ipsecSysd stat  ---> "Running"
cat proc ipcmmd stat  ---> "Running"
cat proc ipmscmm stat  ---> "Running"
cat proc iprm stat  ---> "Running"
cat proc udpRelayCmmd stat  ---> "Running"
Layer3/Switching Processes ---> Ok
Checking Remote Service Process...
cat proc telnetd stat  -------- > "Running"
cat proc sshd stat  -------- > "Running"
cat proc ftpd stat  -------- > "Running"
cat proc httpd stat  -------- > "Running"
cat proc snmpd stat  -------- > "Running"
cat proc ntpd stat  -------- > "Running"
cat proc radius stat  -------- > "Running"
Remote Service Process is OK

Release History

Release 8.3.1; command introduced.
Release 8.8R1; output updated for secureadmin user.

Related Commands

show aaa switch-access
show aaa switch-access hardware-self-test

Displays the major hardware components status.

MIB Objects

N/A
aaa common-criteria admin-state

Enables or disables common criteria mode on the switch.

aaa common-criteria admin-state {enable | disable}

Syntax Definitions

enable | disable    Enables or disables the common criteria mode.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900 X48C4E/V48C8/</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The configuration is applied only after a reload of the switch.
- Please refer to the Preparing and Operation of Common Criteria guide available on the Service and Support website for additional information on Common Criteria implementation.

Examples

-> aaa common-criteria admin-state enable
WARNING: Common Criteria configuration is applied only after reload

Release History

Release 8.3.1; command introduced.

Related Commands

show aaa common-criteria config    Displays the common criteria status on the switch.

MIB Objects

N/A
show aaa common-criteria config

Displays the common criteria status on the switch.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

`-> show aaa common-criteria config`
Admin State: Enabled,
Operational State: Enabled

Release History

Release 8.3.1; command introduced.

Related Commands

`aaa common-criteria admin-state` Enables or disables common criteria mode on the switch.

MIB Objects

N/A
aaa certificate update-ca-certificate

Updates the CA-bundle with the custom CA server certificate provided by CA.

`aaa certificate update-ca-certificate ca_file`

**Syntax Definitions**

`ca_file` The custom CA server certificate (in PEM format) provided by the CA.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The custom CA server certificate should be copied in PEM format to the `/flash/switch/cert.d` directory via SFTP.
- This command appends the existing CA bundle (`certs.pem`) and the custom CA server certificate provided as input.
- The update of custom CA server certificates needs to be done before corresponding server configurations are done on the switch. If the update is done post server configuration, then a switch reboot needs to be done for the changes to take effect.

**Examples**

```
-> aaa certificate update-ca-certificate ca.pem
```

**Release History**

Release 8.3.1; command introduced.
Related Commands

**aaa certificate update-crl**  Updates the CRL list with the custom CRL provided by CA.

MIB Objects

N/A
aaa certificate update-crl

Updates the CRL list with the custom CRL provided by CA.

```bash
aaa certificate update-crl crl_file
```

### Syntax Definitions

**crl_file**

The custom CRL file (in PEM format) provided by the CA.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The custom CRL file should be copied in PEM format to the `/flash/switch/cert.d` directory via SFTP.
- This command appends the existing CRL file (`crl.pem`) and the custom CRL provided as input.
- The update of the custom CRL needs to be done before corresponding server configurations are done on the switch. If the update is done post server configuration, then a switch reboot needs to be done for the changes to take effect.

### Examples

```bash
-> aaa certificate update-crl crl.pem
```

### Release History

Release 8.3.1; command introduced.

### Related Commands

- **aaa certificate update-ca-certificate**
  
  Updates the CA-bundle with the custom CA server certificate provided by CA.

### MIB Objects

N/A
aaa certificate generate-rsa-key key-file

Generates the RSA 2048 bit key with the file name provided as input.

**Syntax Definitions**

`key_file` The name of the key file under which the RSA 2048 bit key is stored.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 6900</th>
<th>6900 6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Generates RSA 2048 bit key in `/flash/switch/cert.d` directory with the file name as the input key file.

**Examples**

```
-> aaa certificate generate-rsa-key key-file myCliPrivate.key
```

**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `aaa certificate generate-self-signed` Generates the X.509 self-signed certificate for TLS client authentication.
- `aaa certificate view` Displays the contents of the X.509 certificate.
- `aaa certificate delete` Deletes the X.509 certificate.

**MIB Objects**

N/A
aaa certificate generate-self-signed

Generates the X.509 self-signed certificate for TLS client authentication.

```
aaa certificate generate-self-signed {cert_file} key {key_file} [days valid_period] {cn common_name} {on org_name} {ou org_unit} {l locality} {st state} {c country}
```

### Syntax Definitions

- **cert_file**
  - The name of the X.509 certificate file to be created.

- **key_file**
  - The name of the key file under which the RSA 2048 bit key is stored.

- **valid_period**
  - Validity period (in days) of the X.509 certificate.

- **common_name**
  - Common Name used in X.509 certificate.

- **org_name**
  - The Organization Name used in X.509 certificate.

- **org_unit**
  - The Organization Unit used in X.509 certificate.

- **locality**
  - The Locality used in X.509 certificate.

- **state**
  - The State used in X.509 certificate.

- **country**
  - The Country used in X.509 certificate.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command generates the file in `/flash/switch/cert.d` directory.

- Default values will be taken for all other optional parameters while generating the X.509 certificate.

- The X.509 certificate needs to be done before corresponding server configurations are done on the switch. If the certificate is created post server configuration, then a switch reboot needs to be done for the changes to take effect.

### Examples

```
-> aaa certificate generate-self-signed myCliCert.pem key clientkey.key days 3650 cn client.ale.com on ALE ou ESD l BAN st KAR c IN
```
**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `aaa certificate generate-rsa-key`  
  
  Generates the RSA 2048 bit key with the file name provided as input.

- `aaa certificate view`  
  
  Displays the contents of the X.509 certificate.

- `aaa certificate delete`  
  
  Deletes the X.509 certificate.

**MIB Objects**

N/A
aaa certificate view

Displays the contents of the X.509 certificate.

aaa certificate view cert_file

Syntax Definitions

**cert_file**

The X.509 certificate file (in PEM format) to be displayed.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> aaa certificate view clientcert.pem
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=client.ale.com , O=ale , OU=esd , L=bn , ST=kar , C=in
    Validity
      Not Before: Jan 3 23:09:07 2014 GMT
      Not After : Jan 1 23:09:07 2024 GMT
    Subject: CN=client.ale.com , O=ale , OU=esd , L=bn , ST=kar , C=in
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        1b:62:al:04:2b:55:c4:2e:9b:8a:48:e0:3a:e0:be:
AAA Commands

aaa certificate view

Exponent: 65537 (0x10001)

X509v3 extensions:

- Subject Key Identifier:

X509v3 Authority Key Identifier:


X509v3 Basic Constraints:

- CA: TRUE

Signature Algorithm: sha256WithRSAEncryption

-----BEGIN CERTIFICATE-----

MIIDlzCCAn+gAwIBAgIJAM+PEWMj1Cj2MA0GCSqGSIb3DQEBCwUAMGIXgDAMBgNV
BAMMD2NsaWVudc5hbG93dXJhYWwzLjEwMzAbBgNVBAMMEUNoYWxldGV1
MjIwMTcwNzEwMB4wCQYDVQQGEwJQXGQwHhcNMTIwMzEwMTcwNzEw
sha256WithRSAEncryption

e7:12:c0:fe:c8:fe:2c:0f:0c:72:5c:6c:8f:17:bb:0d:25:e4:
88:81:8b:-----BEGIN CERTIFICATE-----

MII...-----END CERTIFICATE-----

---END CERTIFICATE---
**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `aaa certificate generate-self-signed` Generates the X.509 self-signed certificate for TLS client authentication.
- `aaa certificate delete` Deletes the X.509 certificate.

**MIB Objects**

N/A
aaa certificate verify ca-certificate

Verifies the contents of the X.509 certificate.

`aaa certificate verify ca-certificate ca_cert_file certificate cert_file`

### Syntax Definitions

- **ca_cert_file**: The X.509 certificate file (in PEM format) to be displayed.
- **cert_file**: The X.509 certificate file (in PEM format) to be displayed.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> aaa certificate verify ca-certificate ca_cert certificate cert_file
```

### Release History

Release 8.3.1; command introduced.

### Related Commands

- **aaa certificate generate-self-signed**: Generates the X.509 self-signed certificate for TLS client authentication.
- **aaa certificate delete**: Deletes the X.509 certificate.

### MIB Objects

N/A
aaa certificate delete

Deletes the X.509 certificate.

aaa certificate delete cert_file

---

**Syntax Definitions**

cert_file The X.509 certificate file (in PEM format) to be deleted.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

-> aaa certificate delete clientcert.pem

---

**Release History**

Release 8.3.1; command introduced.

---

**Related Commands**

- **aaa certificate generate-self-signed** Generates the X.509 self-signed certificate for TLS client authentication.
- **aaa certificate view** Displays the contents of the X.509 certificate.

---

**MIB Objects**

- N/A
aaa certificate generate-csr

Generates the CSR (Certificate Signing Request) to be sent to get a CA signed certificate for TLS client authentication.

```bash
aaa certificate generate-csr {csr_file} key {key_file} [dn domain_name] {cn common_name} {on org_name} {ou org_unit} {l locality} {st state} {c country}
```

**Syntax Definitions**

- `csr_file` The name of the CSR certificate file to be created.
- `key_file` The name of the key file under which the RSA 2048 bit key is stored.
- `domain_name` Domain name to be used in the CSR.
- `common_name` Common Name used in X.509 certificate.
- `org_name` The Organization Name used in X.509 certificate.
- `org_unit` The Organization Unit used in X.509 certificate.
- `locality` The Locality used in X.509 certificate.
- `state` The State used in X.509 certificate.
- `country` The Country used in X.509 certificate.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Generates `<csr_file>.pem` file in `/flash/switch` directory. The `<csr_file>.pem` file created should be sent to CA signing authority to get the CA certificate.
- Default values will be taken for all other optional parameters while generating the CSR.
- The CSR needs to be created, sent to CA authority and the corresponding CA certificate (obtained from CA authority) should be uploaded to the `/flash/switch` directory before corresponding server configurations are done on the switch. If the CA certificate is uploaded post server configuration, then a switch reboot needs to be done for the changes to take effect.

**Examples**

```bash
-> aaa certificate generate-csr myCliCert.pem key clientkey.key cn client.ale.com
```
AAA Commands

**aaa certificate generate-csr**

**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- `show aaa common-criteria config`
  Displays the common criteria status on the switch.

**MIB Objects**

- **N/A**
ssl pki client validate-certificate admin-state

Enables or disables the server’s certification validation when the application on the switch acts as TLS client.

ssl pki client validate-certificate admin-state {enable | disable}

**Syntax Definitions**

**enable**
Enables the server’s certification validation for the client application on the switch.

**disable**
Disables the server’s certification validation for the client application on the switch.

**Defaults**
By default, the feature is disabled.

**Platforms Supported**
This command is supported on the following OmniSwitch platforms:

| 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 V72/C32 | 6900 X48C6/T48C6/ | 9900 |
|------|------|------|-------|------|-------|------|------|-------------| X48C8/C32/ |       |
| Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes         | T48C8/     | Yes   |
|      |      |      |       |      |       |      |      |             | C32E/T24C2/ |       |
|      |      |      |       |      |       |      |      |             | X24C2      |       |

**Usage Guidelines**

- When the feature is enabled or disabled, the switch must be rebooted for the changes to be applied.
- When the feature is enabled, TLS client (LDAP, RADIUS, and SYSLOG) applications validate server certificate based on:
  - TLS mutual authentication using X.509 certificates.
  - The presented identifier must match the reference identifier as per RFC 6125 Section 6.
  - X.509 certificate validation using OCSP and CRL.

**Examples**

-> ssl pki client validate-certificate admin-state enable
-> ssl pki client validate-certificate admin-state disable

**Release History**

Release 8.6R1; command introduced.
Related Commands

show ssl pki config
   Displays the Public Key Infrastructure (PKI) configuration.

MIB Objects

systemSslPki
   systemSslPkiClientCertificateValidation
ssl pki client mutual-authentication admin-state

Enables or disables the mutual authentication for the TLS client applications on the switch.

ssl pki client mutual-authentication admin-state {enable | disable}

---

### Syntax Definitions

- **enable**: Enables the mutual authentication for the TLS client applications on the switch. When mutual-authentication is enabled, TLS client applications will need to load `myCliCert.pem`, `myCliPrivate.key` files in `/flash/switch/cert.d` and provide the certificate to server.

- **disable**: Disables the mutual authentication for the TLS client applications on the switch.

---

### Defaults

By default, the feature is disabled.

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- When the feature is enabled or disabled, the switch must be rebooted for the changes to be applied.

- Enable this feature when the TLS client (LDAP, RADIUS, SYSLOG) applications needs to load the certificate `myCliCert.pem` and `myCliPrivate.key` file in `/flash/switch/cert.d` directory and provide the certificate file to server while establishing TLS connection.

- If the server certificate does not meet the validation criteria, the TLS client application connection is terminated.

---

### Examples

```
-> ssl pki client mutual-authentication admin-state enable
-> ssl pki client mutual-authentication admin-state disable
```

---

### Release History

Release 8.6R1; command introduced.
**Related Commands**

- `show ssl pki config`  
  Displays the Public Key Infrastructure (PKI) configuration.

- `ssl pki server mutual-authentication admin-state`  
  Enables or disables the mutual authentication for the TLS server applications on the switch.

- `aaa certificate update-ca-certificate`  
  Updates the CA-bundle with the custom CA server certificate provided by CA.

**MIB Objects**

- `systemSslPkiClientMutualAuthentication`
**ssl pki server mutual-authentication admin-state**

Enables or disables the mutual authentication for the TLS server applications on the switch.

`ssl pki server mutual-authentication admin-state {enable | disable}`

---

**Syntax Definitions**

- **enable**
  
  Enables the mutual authentication for the TLS server applications on the switch. When mutual-authentication is enabled, the TLS server (SNMP) application will require clients to provide their certificate to server while establishing TLS connection.

- **disable**
  
  Disables the mutual authentication for the TLS server applications on the switch.

---

**Defaults**

By default, the feature is disabled.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- When the feature is enabled or disabled, the switch must be rebooted for the changes to be applied.
- Enable this feature when the TLS server (SNMP) application must require clients to provide their certificate to server while establishing TLS connection.
- When the feature is enabled, TLS server (SNMP) application validates client certificate based on:
  - TLS mutual authentication using X.509 certificates.
  - The presented identifier must match the reference identifier as per RFC 6125 Section 6.
  - X.509 certificate validation using OCSP and CRL.
- If the client certificate does not meet the validation criteria, the TLS server application connection is terminated.

---

**Examples**

- `-> ssl pki server mutual-authentication admin-state enable`
- `-> ssl pki server mutual-authentication admin-state disable`
**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- `show ssl pki config` Displays the Public Key Infrastructure (PKI) configuration.
- `ssl pki client mutual-authentication admin-state` Enables or disables the mutual authentication for the TLS client applications on the switch.

**MIB Objects**

- `systemSslPki`
- `systemSslPkiServerMutualAuthentication`
**ssl pki tls version**

Configures the TLS version for both TLS client and server applications.

ssl pki tls version {1.0 | 1.1 | 1.2}

---

**Syntax Definitions**

1.0  
Sets the TLS version for client and server to 1.0.

1.1  
Sets the TLS version for client and server to 1.1.

1.2  
Sets the TLS version for client and server to 1.2.

**Defaults**

By default, the SSL PKI TLS version is 1.0.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The switch must be rebooted for the changes to be applied.
- When the TLS version is configured, TLS client and server applications will deny all SSL and TLS versions which are lower than the configured version.
- The command is applicable only for LDAP, RADIUS, SYSLOG and SNMP applications.

**Examples**

- `ssl pki tls version 1.0`
- `ssl pki tls version 1.2`

**Release History**

Release 8.6R1; command introduced.
Related Commands

show ssl pki config

Displays the Public Key Infrastructure (PKI) configuration.

MIB Objects

systemSslPki
  systemSslPkiTlsVersion
**show ssl pki config**

Displays the Public Key Infrastructure (PKI) configuration.

**show ssl pki config**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>6900 X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ssl pki config
SSL PKI Global Configuration:
Client Validate Certificate = enabled
Client Mutual Authentication = enabled
Server Mutual Authentication = enabled
TLS version = 1.2
```

**Release History**

Release 8.6R1; command introduced.
**Related Commands**

- `ssl pki client validate-certificate admin-state` Enables or disables the server’s certification validation when the application on the switch acts as client.
- `ssl pki client mutual-authentication admin-state` Enables or disables the mutual authentication for the TLS client applications on the switch.
- `ssl pki server mutual-authentication admin-state` Enables or disables the mutual authentication for the TLS server applications on the switch.
- `ssl pki tls version` Configures the TLS version for both TLS client and server applications.

**MIB Objects**

- `systemSslPki
  - systemSslPkiClientCertificateValidation
  - systemSslPkiClientMutualAuthentication
  - systemSslPkiServerMutualAuthentication
  - systemSslPkiTlsVersion`
### ssl cipher

Selects the cipher security level for the applications using the OpenSSL.

```
ssl cipher {[level {all | high | medium | low}] | [custom {string | file string}]}
```

#### Syntax Definitions

- **all**
  - Includes all the cipher suites, including NULL-SHA.

- **high**
  - Includes only AES-256 with SHA-2 ciphers (Applicable only for TLSv1.2).

- **medium**
  - Includes all ciphers suites, except NULL-SHA, DES-CBC-SHA, and RC4-MD5.

- **low**
  - Includes all cipher suites, except NULL-SHA.

- **string**
  - Name of the cipher suite. It can be list of ciphers or a collective cipher file name. The custom cipher can have a maximum length of 255 characters in CLI and the cipher file can be of maximum 1024 bytes in size.

#### Defaults

By default, the SSL cipher security level is set to medium in default switch operation mode and high in common criteria mode.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- To apply the new SSL cipher security level, switch must be rebooted.

- The command is applicable only for LDAP, Syslog, RADIUS, SNMP, and Captive Portal applications.

- Custom ciphers cannot be more than 255 characters. Hence, the cipher files can be used to configure ciphers more than 255 characters.

- The cipher file can be created by copying the required ciphers in the notepad and saving it as a cipher file with “.cipher” as the file extension.

- The ciphers for the custom cipher and cipher file must be from the supported list of ciphers. To view the supported ciphers, use the `show ssl ciphers all` command.

- The cipher file must be copied to the flash directory of the switch before using this command.
• In chassis based model, the cipher file needs to be copied in both the primary and secondary unit flash directory. In VC based models, the cipher file must be copied to all the flash directory of all the modules.

Examples

-> ssl cipher level all  
-> ssl cipher level low  
-> ssl cipher level medium  
-> ssl cipher level high  
-> ssl cipher custom AECDH-AES256-SHA  
-> ssl cipher custom file /flash/abc.cipher

Release History

Release 8.6R1; command introduced.

Related Commands

show ssl ciphers all  
show ssl ciphers config  

Displays all the supported OpenSSL ciphers.

Displays the current cipher security level configuration.

MIB Objects

SSLCipherSuiteTable
  systemSslCipherLevel  
  systemSslCipherSuite
**show ssl ciphers all**

Displays all the supported OpenSSL ciphers.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
AAA Commands

show ssl ciphers all


Release History

Release 8.6R1; command introduced.

Related Commands

ssl pki client validate-certificate admin-state

Allows to select the cipher security level for the applications using the OpenSSL.

show ssl ciphers config

Displays the current cipher security level configuration.

MIB Objects

SSLCipherSuiteTable

systemSslCipherSuite
show ssl ciphers config

Displays the current cipher security level configuration.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ssl ciphers config
   SSL Cipher Global Configuration:
   SSL Cipher Level = medium
   SSL Cipher Suite = ALL:eNULL:!NULL-SHA:!DES-CBC-SHA:!RC4-MD5

-> show ssl ciphers config
   SSL Cipher Global Configuration:
   SSL Cipher Level = custom-file
   SSL Cipher Suite File = /flash/abc.cipher

Release History

Release 8.6R1; command introduced.
**Related Commands**

- **ssl pki client validate-certificate admin-state**
  - Allows to select the cipher security level for the applications using the OpenSSL.

- **show ssl ciphers all**
  - Displays all the supported OpenSSL ciphers.

**MIB Objects**

- SSLCipherSuiteTable
  - systemSslCipherSuite
**kerberos inactivity-timer**

Configures global inactivity timer on the switch for Kerberos users.

`kerberos inactivity-timer num`

---

**Syntax Definitions**

`num` Time interval in minutes.

---

**Defaults**

By default, inactivity timer is set to 300 minutes.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The valid range of inactivity timer is 10–600 minutes.
- Whenever a Kerberos user becomes inactive, then the inactivity timer will be started for that user. If Kerberos user becomes active before inactivity timer expiry, then timer will be stopped. User entry will be removed from the Kerberos user database on timer expiry.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

---

**Examples**

`-> kerberos inactivity-timer 30`

---

**Release History**

Release 8.6R2; command introduced.
Related Commands

**kerberos server-timeout**
Configures global server reply time-out timer value on the switch for Kerberos users.

**show kerberos configuration**
Displays Kerberos global configuration.

MIB Objects

alaDaKerberosGlobalConfig

alaDaKerberosGlobalInactivityTimer
**kerberos ip-address**

Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.

```
kerberos ip-address ip_address [port num]
no kerberos ip-address ip_address
```

**Syntax Definitions**

`ip_address`  
The IP address of the Kerberos server. (KDC)

`num`  
UDP or TCP port number of the Kerberos application running on the Kerberos server. UDP port range is 1–65535.

**Defaults**

Default value of the port is 88.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- At least one Kerberos server and one Kerberos enabled port must be configured on the switch for Kerberos snooping to function.
- A maximum of two Kerberos server IP addresses can be configured on a switch
- Server IP address cannot be configured as 0.0.0.0, and the octet value in the IP address cannot be greater than 255 (for example, 1.256.2.3).
- Use the `port` keyword to configure both UDP and TCP protocol port number.
- Use the `no` form of this command to delete the Kerberos server IP address. Only one server can be deleted at a time.
- The UDP/TCP port number is not required to remove the Kerberos server IP address configuration.
- If all the authentication servers are removed from the switch, then all the Kerberos users learned so far on all the ports are not removed from the database.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.
**Examples**

-> kerberos ip-address 172.21.160.102 port 2001  
-> kerberos ip-address 172.21.160.103 port 2003  
-> no kerberos ip-address 172.21.160.102

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

- **kerberos inactivity-timer**: Configures a global inactivity timer on the switch for Kerberos users.

- **kerberos server-timeout**: Configures a global server reply time-out timer value on the switch for Kerberos users.

- **show kerberos configuration**: Displays the Kerberos global configuration.

**MIB Objects**

- alaDaKerberosServerTable  
- alaKerberosIpAddress  
- alaDaKerberosUdpPort  
- alaDaKerberosRowStatus
**kerberos server-timeout**

Configures global server reply time-out timer value on the switch for Kerberos users.

```
kerberos server-timeout seconds
```

**Syntax Definitions**

- `seconds` Server reply time-out time interval in seconds in the range 1 second to 30 seconds.

**Defaults**

By default, reply-timeout is 2 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- All the users trying to get authenticated from a specific server will have the same value for reply-timeout timer.
- Whenever a Kerberos request packet is sent to the server, the server reply time-out starts. If the timer expires before receiving the reply from the server, the user authentication is marked as server-time-out and a trap is generated.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

**Examples**

```
-> kerberos server-timeout 20
```

**Release History**

Release 8.6R2; command introduced.
Related Commands

**show kerberos configuration**

Displays Kerberos global configuration.

MIB Objects

alaDaKerberosGlobalConfig

alaDaKerberosGlobalServerTimeoutTimer
**kerberos authentication-pass policy-list-name**

Configures a global classification QoS policy list on the switch for Kerberos users.

```
kerberos authentication-pass policy-list-name policy_list
no kerberos authentication-pass policy-list-name
```

### Syntax Definitions

- `policy_list`: Name of the QoS policy list.

### Defaults

By default, there is no Kerberos global QoS policy list configured.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The QoS policy list must be created prior to this configuration.
- Per-user Kerberos policy list configuration is not supported.
- Use the `no` form of this command to remove the global classification QoS policy list from the switch.
- There is no validation done for QoS policy list in Kerberos. It is the user’s responsibility to associate the correct QoS policy list with Kerberos.
- If the QoS policy list is deleted from the system, then the corresponding configuration in Kerberos will be removed and no error message will be thrown.
- If a domain level policy list is configured in the switch and any user belonging to that domain gets authenticated from the Kerberos server, then the domain level policy list is applied to the user over the global policy list.
- If a user gets authenticated from the Kerberos server and the domain level policy list is not configured on the switch for the authenticated user, then the global policy list is applied to the user if the global policy list is configured on the switch.
- If a user gets authenticated from the Kerberos server and neither the domain level policy list (for that user domain) nor the global policy list is configured, then the user traffic is classified on the basis of already applied non-supplicant authentication classification.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
• On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

**Examples**

-> kerberos authentication-pass policy-list-name p2

The following example shows that the p2 is configured as the global classification QoS policy list on the switch for Kerberos users.

-> show kerberos configuration

Inactivity Timer :30 (mins),
Server Timeout :20 (secs),
**Global QoS Policy List** :p2,

Servers :
IP-Address UDP Port
------------------+----------------
1.1.1.1           88

Per Domain QoS policy List :
Domain-Name Policy-List-Name
---------------------------------+--------------------------+--
EXAMPLE.COM       p11

When the QoS policy list p2 is removed from the system, the corresponding configuration in Kerberos is shown as below.

-> no policy list p2
-> qos apply

-> show kerberos configuration

Inactivity Timer :30 (mins),
Server Timeout :20 (secs),

Servers :
IP-Address UDP Port
------------------+----------------
1.1.1.1           88

Per Domain QoS policy List :
Domain-Name Policy-List-Name Status
---------------------------------+--------------------------+----------
EXAMPLE.COM       p11 active

The following command removes the global classification QoS policy list from the switch:

-> no kerberos authentication-pass policy-list-name

**Release History**

Release 8.6R2; command introduced.
Related Commands

**kerberos ip-address**

Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.

**kerberos authentication-pass domain**

Configures "per domain" classification policy for the Kerberos users.

**show kerberos configuration**

Displays Kerberos global configuration.

MIB Objects

<table>
<thead>
<tr>
<th>Object Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaDaKerberosGlobalConfig</td>
</tr>
<tr>
<td>alaDaKerberosGlobalPolicy</td>
</tr>
</tbody>
</table>
**kerberos authentication-pass domain**

Configures a per-domain classification policy for the Kerberos users.

```bash
kerberos authentication-pass domain domain_name policy-list-name policy_list
```

```bash
no kerberos authentication-pass domain domain_name
```

**Syntax Definitions**

- **domain_name**: Domain name on which the QoS policy is applied. Domain name length can be a maximum of 32 characters. Domain name is case sensitive.

- **policy_list**: Name of the QoS policy list already configured.

**Defaults**

By default, there is no Kerberos global QoS policy list configured.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the per-domain classification policy for Kerberos users.
- Domain name is case sensitive.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

**Examples**

```bash
-> kerberos authentication-pass domain EXAMPLE.COM policy-list-name p11
```

The following example shows that the `p11` is configured as the policy list associated with the domain `EXAMPLE.COM`:

```bash
-> show kerberos configuration
Inactivity Timer :30 (mins),
Server Timeout   :20 (secs),

Servers:
IP-Address UDP Port
------------------------+----------
1.1.1.1              88
```

---

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 39-199
Per Domain QoS policy List :
Domain-Name                                      Policy-List-Name
---------------------------------------------------------------
EXAMPLE.COM                                        p11

When the QoS policy list **p11** is removed from the system, the corresponding configuration in Kerberos is shown as below.

-> no policy list p11
-> qos apply
-> show kerberos configuration
Inactivity Timer :30 (mins),
Server Timeout   :20 (secs),

Servers :
IP-Address        UDP Port
-----------------+----------------
1.1.1.1           88

Per Domain QoS policy List :
Domain-Name                                      Policy-List-Name
---------------------------------------------------------------
EXAMPLE.COM                                        p11

The following command removes the per-domain classification policy for Kerberos users:

-> no kerberos authentication-pass domain EXAMPLE.COM

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

**kerberos authentication-pass policy-list-name** Configures global classification QoS policy list on the switch for Kerberos users.

**show kerberos configuration** Displays Kerberos global configuration.

**MIB Objects**

alaDaKerberosPolicyConfigTable
alaDaKerberosPolicyName
alaDaKerberosPolicyRowStatus
clear kerberos statistics

Clears Kerberos statistics.

clear kerberos statistics

**Syntax Definitions**

N/A

**Defaults**

By default, global statistics are cleared.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to clear global Kerberos statistics.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

**Examples**

`-> clear kerberos statistics`

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

- `show kerberos configuration` Displays Kerberos global configuration.

**MIB Objects**

- `alaKerberosGlobalClearStats`
**show kerberos configuration**

Displays Kerberos global configuration.

**show kerberos configuration**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to display information about Kerberos settings configured through the `kerberos inactivity-timer` command.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

**Examples**

```
-> show kerberos configuration

Inactivity Timer : 30 (mins),
Server Timeout : 9 (secs),
Global QoS Policy List : p2,

Servers :
IP-Address         UDP Port
-----------------+-----------------+-
1.2.3.5           90
4.5.6.7           88
11.22.33.55       80

Per Domain QoS policy List :
Domain-Name         Policy-List-Name     Status
-----------------+-----------------+-------------
```
AAA Commands  

Example.com  
pl1  
Active

output definitions

<table>
<thead>
<tr>
<th>Inactivity Timer</th>
<th>Global inactivity timer configured on the switch for Kerberos users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Timeout</td>
<td>Global server reply time-out timer value configured on the switch for Kerberos users.</td>
</tr>
<tr>
<td>Global QoS Policy List</td>
<td>Global classification QoS policy list associated with the Kerberos users</td>
</tr>
<tr>
<td>Servers</td>
<td>IP Address: IP address configured of the Kerberos server.</td>
</tr>
<tr>
<td></td>
<td>UDP Port: UDP or TCP port of the Kerberos application running on the Kerberos server.</td>
</tr>
<tr>
<td>Per Domain QoS policy List</td>
<td>Domain-Name: Per-domain classification policy configured for Kerberos users.</td>
</tr>
<tr>
<td></td>
<td>Policy-List-Name: Name of the QoS policy list associated with the domain.</td>
</tr>
<tr>
<td></td>
<td>Status: Per-domain QoS policy list status (Active or Inactive).</td>
</tr>
<tr>
<td></td>
<td>Inactive status indicates that the policy list does not exist in the switch or the policy list exists, but is not applied.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R2; command introduced.

Related Commands

kerberos inactivity-timer  
Configures global inactivity timer on the switch for Kerberos users.

kerberos ip-address  
Configures IP address of the Kerberos server (Key Distribution Centre - KDC) and UDP or TCP port number.

kerberos server-timeout  
Configures global server reply time-out timer value on the switch for Kerberos users.

kerberos authentication-pass policy-list-name  
Configures global classification QoS policy list on the switch for Kerberos users.

kerberos authentication-pass domain  
Configures per-domain classification policy for the Kerberos users.

show kerberos users  
Displays the learned Kerberos users information.

show kerberos statistics  
Displays the global Kerberos statistics.

clear kerberos statistics  
Clears global Kerberos statistics.

MIB Objects

alaDKerberosGlobalConfig
alaKerberosGlobalInactivityTimer
alaKerberosGlobalServerTimeoutTimer
alaKerberosGlobalPolicy
alaKerberosServerTable
alaKerberosIpAddress
alaKerberosUdpPort
AAA Commands

show kerberos configuration

alaKerberosPolicyConfigTable
  alaKerberosPolicyDomainName
  alaKerberosPolicyName
**show kerberos users**

Displays the learned Kerberos users information.

```
show kerberos users [port chassis/slot/port | linkagg agg_id | mac-address mac_address | count]
```

### Syntax Definitions

- **chassis**: The Chassis Identifier.
- **slot/port**: The slot number for the module and the physical port number on that module (for example, 3/1 specifies port 1 on slot 3).
- **agg_id**: Enter a link aggregate ID number.
- **mac_address**: MAC address of the Kerberos user.
- **count**: Displays the number of Kerberos users.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If a **chassis/slot/port** is specified, the Kerberos users learned on that port are displayed.
- If **agg_id** is specified, the Kerberos users learned on that link aggregate are displayed.
- If a MAC address is specified, then the information related to that Kerberos user is displayed.
- If none of the parameters are specified (chassis/slot/port, MAC address), then the information related to all the Kerberos users learned on the switch is displayed.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

### Examples

```
-> show kerberos users
<table>
<thead>
<tr>
<th>Port</th>
<th>Username</th>
<th>MAC Address</th>
<th>Auth Status</th>
<th>QOS Policy</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1/18 root/admin</td>
<td>00:11:22:33:44:55</td>
<td>tgs-authenticated</td>
<td>p11</td>
<td>AP01.ORG</td>
<td></td>
</tr>
<tr>
<td>2/1/19 guest</td>
<td>00:01:02:03:04:05</td>
<td>tgs-timeOut</td>
<td></td>
<td>AP01.ORG</td>
<td></td>
</tr>
</tbody>
</table>
```
-> show kerberos users port 2/1/18

<table>
<thead>
<tr>
<th>Port</th>
<th>Username</th>
<th>MAC Address</th>
<th>Auth Status</th>
<th>QOS Policy</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1/18</td>
<td>root/admin</td>
<td>00:11:22:33:44:55</td>
<td>tgs-authenticated</td>
<td>pl1</td>
<td>AP01.ORG</td>
</tr>
</tbody>
</table>


AAA Commands

show kerberos users

---

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The Kerberos chassis, slot, and port number.</td>
</tr>
<tr>
<td>Username</td>
<td>User name of the client.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>MAC address of the Kerberos user.</td>
</tr>
<tr>
<td>Auth Status</td>
<td>Kerberos authentication process involves exchange of two requests (AS_REQ and AS_REP) and two response (AS_REP and TGS_REP). This field indicates up to which level the authentication has reached. On successful authentication, &quot;tgs-authenticated&quot; is displayed.</td>
</tr>
<tr>
<td>QoS Policy</td>
<td>QoS policy list configured on the switch for the Kerberos user.</td>
</tr>
<tr>
<td>Domain</td>
<td>Per-domain classification policy configured for the Kerberos user.</td>
</tr>
</tbody>
</table>

```
-> show kerberos users mac-address 00:11:22:33:44:55
```

**Detail User Information:**

- MAC Address: 00:11:22:33:44:55
- Port: 1/1/1
- Authentication Status: tgs-authenticated
- QoS Policy: pl1
- Domain Name: EXAMPLE.COM
- User Name: root\admin
- User Entry State: active
- Inactivity Timer Left: NA

---

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>MAC address of the Kerberos user.</td>
</tr>
<tr>
<td>Port</td>
<td>The Kerberos chassis, slot, and port number.</td>
</tr>
<tr>
<td>Authentication Status</td>
<td>Kerberos authentication process involves exchange of two requests (AS_REQ and AS_REP) and two response (AS_REP and TGS_REP). This field indicates up to which level the authentication has reached. On successful authentication, &quot;tgs-authenticated&quot; is displayed.</td>
</tr>
<tr>
<td>QoS Policy</td>
<td>QoS policy list configured on the switch for the Kerberos user.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Per-domain classification policy configured for the Kerberos user.</td>
</tr>
<tr>
<td>User Name</td>
<td>User name of the client.</td>
</tr>
<tr>
<td>User Entry State</td>
<td>The current state of the user.</td>
</tr>
<tr>
<td>Inactivity Timer Left</td>
<td>The amount of time left, in seconds, of the inactivity timer value.</td>
</tr>
</tbody>
</table>

---

**Release History**

Release 8.6R2; command introduced.
**Related Commands**

- **kerberos authentication-pass policy-list-name** Configures global classification QoS policy list on the switch for Kerberos users.
- **kerberos authentication-pass domain** Configures per-domain classification policy for the Kerberos users.
- **show kerberos configuration** Displays Kerberos global configuration.
- **clear kerberos statistics** Clears global Kerberos statistics.

**MIB Objects**

- alaDaKerberosUserTable
  - alaDaKerberosUserMac
  - alaDaKerberosUserPort
  - alaDaKerberosUserName
  - alaDaKerberosUserDomain
  - alaDaKerberosUserAuthState
  - alaDaKerberosUserPolicy
  - alaDaKerberosUserLeftTime
  - alaDaKerberosUserState
**show kerberos statistics**

Displays global Kerberos statistics.

**show kerberos statistics**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to display the global Kerberos statistics.
- On OS6465 and OS6900, Kerberos is supported only in bridge mode.
- On OS6860N, Kerberos is supported in bridge mode and access port on SPB.

**Examples**

```bash
-> show kerberos statistics
Total Client Packet Rx : 52
Total Server Packet Rx : 13
Total KRB-AS-REQ Packet Rx : 47
Total KRB-AS-REP Packet Rx : 8
Total KRB-TGS-REQ Packet Rx : 5
Total KRB-TGS-REP Packet Rx : 5
Total KRB-ERROR Packet Rx : 0
Total Client Packet Sw Discard : 0
Total Server Packet Sw Discard : 2
```

**output definitions**

- **Total Client Packet Rx**: Total client request packets received.
- **Total Server Packet Rx**: Total server response packets received.
- **Total KRB-AS-REQ Packet Rx**: Total AS-REQ request packets received.
- **Total KRB-AS-REP Packet Rx**: Total AS-REP response packets received.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total KRB-TGS-REQ Packet Rx</td>
<td>Total TGS-REQ request packets received.</td>
</tr>
<tr>
<td>Total KRB-TGS-REP Packet Rx</td>
<td>Total TGS-REP response packets received.</td>
</tr>
<tr>
<td>Total KRB-ERROR Packet Rx</td>
<td>Total error packets received from the server.</td>
</tr>
<tr>
<td>Total Client Packet Sw Discard</td>
<td>Total client's request packets discarded at software by Kerberos module.</td>
</tr>
<tr>
<td>Total Server Packet Sw Discard</td>
<td>Total server's response packets discarded at software by Kerberos module.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.6R2; command introduced.

**Related Commands**

- **show kerberos configuration**
  - Displays Kerberos global configuration.
- **clear kerberos statistics**
  - Clears global and port-level Kerberos statistics.

**MIB Objects**

- alaDaKerberosTotalClientPktRxStats
- alaDaKerberosTotalServerPktRxStats
- alaDaKerberosClientPktSwDiscardStats
- alaDaKerberosServerPktSwDiscardStats
- alaDaKerberosTotalASREQRxStats
- alaDaKerberosTotalASREPRxStats
- alaDaKerberosTotalTGSREQRxStats
- alaDaKerberosTotalTGSREPRxStats
- alaDaKerberosTotalErrorRxStats
aaa jitc admin-state

Enables or disables Joint Interoperability Test Command (JITC) mode on the switch.

```
aaa jitc admin-state {enable | disable}
```

**Syntax Definitions**

```
enable | disable
```

Enables or disables the JITC (Joint Interoperability Test Command) mode.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The configuration is applied only after a reload of the switch.
- The JITC mode is mutually exclusive of Common Criteria mode and Enhanced-mode. If the switch is already running in Common Criteria or enhanced-mode (NIS) it must be disabled before enabling JITC mode and vise versa.

**Examples**

```
-> aaa jitc admin-state enable
WARNING: JITC mode configuration is applied only after reload
```

**Release History**

Release 8.4.1; command introduced.

**Related Commands**

```
show aaa jitc config
```

Displays the JITC status on the switch.

**MIB Objects**

N/A
**show aaa jitc config**

Displays the JITC status on the switch.

```
show aaa jitc config
```

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show aaa jitc config
Admin State: Enabled,
Operational State: Enabled
```

**output definitions**

- **Admin State**: Indicates configuration status of JITC mode (Enabled or Disabled).
- **Operational State**: Indicates operational status of JITC mode (Enabled or Disabled).

**Release History**

Release 8.4.1; command introduced.
Related Commands

**aaa jitc admin-state**
Enables or disables JITC mode on the switch.

MIB Objects

N/A
Access Guardian refers to a set of OmniSwitch security functions that work together to provide a dynamic, proactive network security solution. This chapter provides information about the commands that are used to configure the following Access Guardian features through the Command Line Interface (CLI):

- **Universal Network Profile (UNP)**—Access Guardian is configured and applied through the framework of the UNP feature. UNP is enabled on switch ports to activate Access Guardian functionality that is used to authenticate and classify users into UNP profiles. Each profile is mapped to a VLAN ID or Service Access Point (SAP) to which the user is dynamically assigned. Specific UNP port configurations help to simplify and easily replicate the same configuration across multiple ports.

- **Bring Your Own Device (BYOD) - OmniSwitch / UPAM or ClearPass Integration**: The OmniSwitch leverages Access Guardian functionality along with the OmniVista Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) to provide an overall BYOD solution.
  - Configurable UNP port and profile attributes are used to redirect traffic from the OmniSwitch to the UPAM or CPPM server.
  - Configurable GRE tunnels allow the OmniSwitch to intercept and tunnel Multicast Domain Name System (mDNS) and Simple Service Discovery Protocol (SSDP) packets to or from a WLAN controller in a BYOD network.

- **Captive Portal**—Internal and external Captive Portal Web-based authentication. Internal Captive Portal authentication is provided through an internal Web server on the OmniSwitch that presents default or customized Web pages to the user. A post-authentication and/or post-classification process to validate user credentials and dynamically assign a new role (policy list) to enforce user access to the network. External, guest Captive Portal authentication is provided through the OmniSwitch Access Guardian interaction with the OmniVista Unified Policy Access Manager or the ClearPass Policy Manager.

- **Quarantine Manager and Remediation (QMR)**—QMR is a switch-based application that restricts the network access of known quarantined users and provides a remediation path to allow quarantined users to regain their network access.

- **IoT Device Profiling IoT**—Device Profiling allows the network administrators to support and manage smart phones, Tablets and other devices connecting to the network. The IoT Device Profiling uses DHCP FingerPrinting and MAC OUI (MAC Vendors) to identify IoT devices.

For commands used to configure device authentication, authorization, and accounting parameters that are used to support Access Guardian functionality, see “Chapter 39, “AAA Commands.”

For commands used to configure Learned Port Security (LPS), which is used by Access Guardian to help ensure that only certain devices are allowed to connect to the switch, see “Chapter 47, “Learned Port Security Commands.”
MIB information for the UNP commands is as follows:

- **Filename**: ALCATEL-IND1-DA-MIB.mib
  - **Module**: alcatelIND1DaMIB

- **Filename**: ALCATEL-IND1-UDP-RELAY-MIB.mib
  - **Module**: alcatelIND1UDP RelayMIB

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>UNP Global Configuration Commands</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>unp dynamic-vlan-configuration</td>
</tr>
<tr>
<td></td>
<td>unp dynamic-profile-configuration</td>
</tr>
<tr>
<td></td>
<td>unp delay-learning</td>
</tr>
<tr>
<td></td>
<td>unp auth-server-down</td>
</tr>
<tr>
<td></td>
<td>unp auth-server-down port-bounce</td>
</tr>
<tr>
<td></td>
<td>unp auth-server-down-timeout</td>
</tr>
<tr>
<td></td>
<td>unp policy validity-period</td>
</tr>
<tr>
<td></td>
<td>unp policy validity-location</td>
</tr>
<tr>
<td></td>
<td>unp domain description</td>
</tr>
<tr>
<td></td>
<td>unp redirect port-bounce</td>
</tr>
<tr>
<td></td>
<td>unp redirect pause-timer</td>
</tr>
<tr>
<td></td>
<td>unp redirect proxy-server-port</td>
</tr>
<tr>
<td></td>
<td>unp redirect server</td>
</tr>
<tr>
<td></td>
<td>unp redirect allowed-name</td>
</tr>
<tr>
<td></td>
<td>unp force-l3-learning</td>
</tr>
<tr>
<td></td>
<td>unp 802.1x-pass-through</td>
</tr>
<tr>
<td></td>
<td>unp ipv6-drop</td>
</tr>
<tr>
<td></td>
<td>unp ap-mode</td>
</tr>
<tr>
<td></td>
<td>unp mac-mobility</td>
</tr>
<tr>
<td></td>
<td>unp user flush</td>
</tr>
<tr>
<td></td>
<td>unp 802.1x eapol-version</td>
</tr>
<tr>
<td></td>
<td>unp multi-untag-sap</td>
</tr>
<tr>
<td></td>
<td>show unp global configuration</td>
</tr>
<tr>
<td></td>
<td>show unp domain</td>
</tr>
<tr>
<td></td>
<td>show unp user</td>
</tr>
<tr>
<td></td>
<td>show unp user status</td>
</tr>
<tr>
<td></td>
<td>show unp user details</td>
</tr>
<tr>
<td></td>
<td>show unp policy validity-period</td>
</tr>
<tr>
<td></td>
<td>show unp policy validity-location</td>
</tr>
<tr>
<td>UNP Profile Commands</td>
<td>unp profile</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td></td>
<td>unp profile qos-policy-list</td>
</tr>
<tr>
<td></td>
<td>unp profile location-policy</td>
</tr>
<tr>
<td></td>
<td>unp profile period-policy</td>
</tr>
<tr>
<td></td>
<td>unp profile captive-portal-authentication</td>
</tr>
<tr>
<td></td>
<td>unp profile captive-portal-profile</td>
</tr>
<tr>
<td></td>
<td>unp profile kerberos-authentication</td>
</tr>
<tr>
<td></td>
<td>unp profile authentication-flag</td>
</tr>
<tr>
<td></td>
<td>unp profile mobile-tag</td>
</tr>
<tr>
<td></td>
<td>unp profile maximum-ingress-bandwidth</td>
</tr>
<tr>
<td></td>
<td>unp profile maximum-egress-bandwidth</td>
</tr>
<tr>
<td></td>
<td>unp profile maximum-ingress-depth</td>
</tr>
<tr>
<td></td>
<td>unp profile maximum-egress-depth</td>
</tr>
<tr>
<td></td>
<td>unp profile inactivity-interval</td>
</tr>
<tr>
<td></td>
<td>unp profile mac-mobility</td>
</tr>
<tr>
<td></td>
<td>unp profile saa-profile</td>
</tr>
<tr>
<td></td>
<td>unp profile map vlan</td>
</tr>
<tr>
<td></td>
<td>unp profile map service-type spb</td>
</tr>
<tr>
<td></td>
<td>unp profile map service-type vxlan</td>
</tr>
<tr>
<td></td>
<td>unp vxlan far-end-ip-list</td>
</tr>
<tr>
<td></td>
<td>unp profile map service-type l2gre</td>
</tr>
<tr>
<td></td>
<td>unp l2gre far-end-ip-list</td>
</tr>
<tr>
<td></td>
<td>unp profile map service-type static</td>
</tr>
<tr>
<td></td>
<td>show unp profile</td>
</tr>
<tr>
<td></td>
<td>show unp profile map</td>
</tr>
<tr>
<td></td>
<td>show unp vxlan far-end-ip-list</td>
</tr>
<tr>
<td></td>
<td>show unp l2gre far-end-ip-list</td>
</tr>
<tr>
<td>UNP System Default Profile Commands</td>
<td>unp system-default service-mod</td>
</tr>
<tr>
<td></td>
<td>unp system-default service-base</td>
</tr>
<tr>
<td></td>
<td>unp system-default multicastmode</td>
</tr>
<tr>
<td></td>
<td>unp system-default vlan-xlation</td>
</tr>
<tr>
<td></td>
<td>unp system-default multicastgroup</td>
</tr>
<tr>
<td></td>
<td>unp system-default far-end-ip-list</td>
</tr>
<tr>
<td></td>
<td>show unp global configuration</td>
</tr>
<tr>
<td>UNP SAA Profile Commands</td>
<td>unp saa-profile</td>
</tr>
<tr>
<td></td>
<td>show unp saa-profile</td>
</tr>
<tr>
<td>Device Profiling Commands</td>
<td>device-profile admin-state</td>
</tr>
<tr>
<td></td>
<td>device-profile port linkagg</td>
</tr>
<tr>
<td></td>
<td>device-profile device-type</td>
</tr>
<tr>
<td></td>
<td>device-profile update-signature</td>
</tr>
<tr>
<td></td>
<td>device-profile update-signature from</td>
</tr>
<tr>
<td></td>
<td>device-profile auto-unp-assignment</td>
</tr>
<tr>
<td></td>
<td>show device-profile config</td>
</tr>
<tr>
<td></td>
<td>show device-profile summary</td>
</tr>
<tr>
<td></td>
<td>show device-profile catalog</td>
</tr>
<tr>
<td></td>
<td>show device-profile signatures from</td>
</tr>
<tr>
<td></td>
<td>show device-profile signatures</td>
</tr>
</tbody>
</table>
### UNP Port Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp port-type</td>
<td></td>
</tr>
<tr>
<td>unp l2-profile</td>
<td></td>
</tr>
<tr>
<td>unp redirect port-bounce</td>
<td></td>
</tr>
<tr>
<td>unp 802.1x-authentication</td>
<td></td>
</tr>
<tr>
<td>unp 802.1x-authentication pass-alternate</td>
<td></td>
</tr>
<tr>
<td>unp 802.1x-authentication tx-period</td>
<td></td>
</tr>
<tr>
<td>unp 802.1x-authentication supp-timeout</td>
<td></td>
</tr>
<tr>
<td>unp 802.1x-authentication max-req</td>
<td></td>
</tr>
<tr>
<td>unp 802.1x-authentication bypass-8021x</td>
<td></td>
</tr>
<tr>
<td>unp 802.1x-authentication failure-policy</td>
<td></td>
</tr>
<tr>
<td>unp mac-authentication</td>
<td></td>
</tr>
<tr>
<td>unp mac-authentication pass-alternate</td>
<td></td>
</tr>
<tr>
<td>unp mac-authentication allow-eap</td>
<td></td>
</tr>
<tr>
<td>unp classification</td>
<td></td>
</tr>
<tr>
<td>unp trust-tag</td>
<td></td>
</tr>
<tr>
<td>unp default-profile</td>
<td></td>
</tr>
<tr>
<td>unp domain</td>
<td></td>
</tr>
<tr>
<td>unp aaa-profile</td>
<td></td>
</tr>
<tr>
<td>unp port port-template</td>
<td></td>
</tr>
<tr>
<td>unp direction</td>
<td></td>
</tr>
<tr>
<td>unp admin-state</td>
<td></td>
</tr>
<tr>
<td>unp dynamic-service</td>
<td></td>
</tr>
<tr>
<td>unp vlan</td>
<td></td>
</tr>
<tr>
<td>unp port profile</td>
<td></td>
</tr>
<tr>
<td>unp force-l3-learning</td>
<td></td>
</tr>
<tr>
<td>unp port ap-mode</td>
<td></td>
</tr>
<tr>
<td>show unp port</td>
<td></td>
</tr>
<tr>
<td>show unp port config</td>
<td></td>
</tr>
<tr>
<td>show unp port bandwidth</td>
<td></td>
</tr>
<tr>
<td>show unp port 802.1x statistics</td>
<td></td>
</tr>
<tr>
<td>show unp port configured-vlans</td>
<td></td>
</tr>
<tr>
<td>show unp port profile</td>
<td></td>
</tr>
</tbody>
</table>

### UNP Port Template Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp port-template</td>
<td></td>
</tr>
<tr>
<td>show unp port-template</td>
<td></td>
</tr>
</tbody>
</table>

### Router Domain Authentication

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp network-group</td>
<td></td>
</tr>
<tr>
<td>unp router-auth user-group</td>
<td></td>
</tr>
<tr>
<td>unp router-auth cp-profile</td>
<td></td>
</tr>
<tr>
<td>unp router-auth user flush</td>
<td></td>
</tr>
<tr>
<td>show unp network-group</td>
<td></td>
</tr>
<tr>
<td>show unp router-auth user-group</td>
<td></td>
</tr>
<tr>
<td>show unp router-auth configuration</td>
<td></td>
</tr>
<tr>
<td>show unp router-auth users</td>
<td></td>
</tr>
</tbody>
</table>

### Classification Rule Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp classification port</td>
<td></td>
</tr>
<tr>
<td>unp classification domain</td>
<td></td>
</tr>
<tr>
<td>unp classification mac-address</td>
<td></td>
</tr>
<tr>
<td>unp classification mac-oui</td>
<td></td>
</tr>
<tr>
<td>unp classification mac-range</td>
<td></td>
</tr>
<tr>
<td>unp classification ip-address</td>
<td></td>
</tr>
<tr>
<td>unp classification vlan-tag</td>
<td></td>
</tr>
<tr>
<td>unp classification lldp med-endpoint</td>
<td></td>
</tr>
<tr>
<td>unp classification authentication-type</td>
<td></td>
</tr>
<tr>
<td>show unp classification</td>
<td></td>
</tr>
<tr>
<td>Access Guardian Commands</td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| Extended Classification Rule Commands | unp classification-rule  
unp classification-rule port  
unp classification-rule domain  
unp classification-rule mac-address  
unp classification-rule mac-oui  
unp classification-rule mac-range  
unp classification-rule ip-address  
unp classification-rule vlan-tag  
unp classification-rule lldp med-endpoint  
unp classification-rule authentication-type  
unp classification-rule device-type  
show unp classification-rule |
| User Role Commands | unp user-role  
unp user-role policy-list  
unp user-role profile  
unp user-role authentication-type  
unp user-role cp-status-post-login  
unp restricted-role policy-list  
show unp user-role  
show unp restricted-role |
| Captive Portal Commands | captive-portal mode  
captive-portal name  
captive-portal ip-address  
captive-portal success-redirect-url  
captive-portal proxy-server-port  
captive-portal retry-count  
captive-portal authentication-pass  
captive-portal authentication-pass domain  
captive-portal-profile  
captive-portal customization  
show captive-portal configuration  
show captive-portal profile-names |
| Quarantine Manager and Remediation (QMR) Commands | qmr quarantine path  
qmr quarantine page  
qmr quarantine allowed-name  
qmr quarantine custom-proxy-port  
show qmr  
show quarantine mac group |
<table>
<thead>
<tr>
<th>Zero Configuration Networking Commands (mDNS and SSDP)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>zeroconf mdns admin-state</td>
<td></td>
</tr>
<tr>
<td>zeroconf ssdp admin-state</td>
<td></td>
</tr>
<tr>
<td>zeroconf mode</td>
<td></td>
</tr>
<tr>
<td>zeroconf responder-ip</td>
<td></td>
</tr>
<tr>
<td>zeroconf gateway-vlan-list</td>
<td></td>
</tr>
<tr>
<td>zeroconf access-vlan-list</td>
<td></td>
</tr>
<tr>
<td>zeroconf server-policy</td>
<td></td>
</tr>
<tr>
<td>zeroconf client-policy</td>
<td></td>
</tr>
<tr>
<td>zeroconf service-rule policy</td>
<td></td>
</tr>
<tr>
<td>zeroconf service-rule service-id</td>
<td></td>
</tr>
<tr>
<td>zeroconf service-list</td>
<td></td>
</tr>
<tr>
<td>zeroconf service-id query-request</td>
<td></td>
</tr>
<tr>
<td>zeroconf edge-ip-list</td>
<td></td>
</tr>
<tr>
<td>zeroconf edge-ip-list mode</td>
<td></td>
</tr>
<tr>
<td>zeroconf refresh-database</td>
<td></td>
</tr>
<tr>
<td>show zeroconf</td>
<td></td>
</tr>
<tr>
<td>show zeroconf services</td>
<td></td>
</tr>
<tr>
<td>show zeroconf services-cache</td>
<td></td>
</tr>
<tr>
<td>show zeroconf edge-details</td>
<td></td>
</tr>
<tr>
<td>show zeroconf server policies</td>
<td></td>
</tr>
<tr>
<td>show zeroconf client policies</td>
<td></td>
</tr>
<tr>
<td>show zeroconf service rules</td>
<td></td>
</tr>
<tr>
<td>show zeroconf server policy-instances</td>
<td></td>
</tr>
</tbody>
</table>
unp dynamic-vlan-configuration

Configures the UNP status for dynamic VLAN configuration. When this functionality is enabled and a VLAN mapping is configured with a VLAN ID that does not exist, the switch will dynamically create the necessary VLAN ID.

unp dynamic-vlan-configuration

no unp dynamic-vlan-configuration

Syntax Definitions

N/A

Defaults

By default, dynamic VLAN configuration is disabled.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note. Dynamic VLANs are not saved in the VLAN section of the boot.cfg file. However, the unp commands to enable dynamic VLAN configuration and create a UNP are saved in the UNP section of the boot.cfg file. As a result, the VLAN is created again on the next switch bootup.

- Use the no form of this command to disable dynamic VLAN configuration.
- When dynamic VLAN configuration is disabled, configuring a VLAN mapping with a VLAN ID that does not exist in the switch configuration is not allowed.
- The VLAN status and other port (non-UNP port) assignments for a dynamic UNP VLAN are configurable using standard VLAN commands. In addition, the STP status is configurable and enabled by default when the dynamic VLAN is created.
- A dynamic VLAN cannot be deleted using standard VLAN commands (no vlan vlan_id).
- UNP dynamic VLANs are identified as a separate type of VLAN. The show vlan command will display this type with the default name of “UNP-DYN-VLAN” and the designated type as “UNP Dynamic Vlan”.

Examples

-> unp dynamic-vlan-configuration
-> no unp dynamic-vlan-configuration

**Release History**

Release 7.2.1; command was introduced.

**Related Commands**

- **unp profile**  
  Configures a UNP in the switch configuration.

- **show unp global configuration**  
  Displays the dynamic VLAN configuration status for the switch.

**MIB Objects**

alaDaUNPGlobalConfiguration
  alaDaUNPDynamicVlanConfigFlag
**unp dynamic-profile-configuration**

Configures the UNP status for dynamic profile configuration. When this functionality is enabled, a UNP profile is dynamically created based on specific traffic conditions.

```
unp dynamic-profile-configuration
no unp dynamic-profile-configuration
```

**Syntax Definitions**

N/A

**Defaults**

By default, dynamic profile configuration is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable dynamic profile configuration.
- When dynamic profile configuration is enabled, a UNP profile is dynamically created when the trust VLAN tag option is enabled on the UNP port or link aggregate and one of the following conditions occurs:
  - A tagged packet received on the UNP port contains a VLAN tag that matches an existing MVRP VLAN in the switch configuration that is not assigned to a profile.
  - There is no matching VLAN in the switch configuration.
- Dynamically created profiles are saved in the `boot.cfg` file for the switch.
- By default, dynamically created profiles are automatically named `dynamic_profile_vlan_id`, where the VLAN ID is the ID of the VLAN contained in the packet tag.
- After the dynamic profile is created, changing the profile name, the associated VLAN ID, or the QoS policy list is allowed. To avoid any confusion, change the profile name if the VLAN ID associated with the profile has changed.
- If the dynamic profile configuration option is enabled along with the dynamic VLAN configuration option and a dynamically created profile refers to a VLAN that is an MVRP VLAN, then the MVRP VLAN is automatically converted to a dynamic UNP VLAN (UNP-DYN-VLAN).
Examples

-> unp dynamic-profile-configuration
-> no unp dynamic-profile-configuration

Release History

Release 7.2.1.R02; command was introduced.

Related Commands

- **unp profile**
  Configures a UNP in the switch configuration.

- **unp dynamic-vlan-configuration**
  Configures the status of dynamic VLAN configuration. When enabled, UNP will create a VLAN at the time a VLAN mapping for a profile is created that specifies a VLAN ID that does not exist in the switch configuration.

- **show unp global configuration**
  Displays the dynamic profile configuration status for the switch.

MIB Objects

- **alaDaUNPGlobalConfiguration**
- **alaDaUNPDynamicProfileConfigFlag**
**unp delay-learning**

Configures the UNP delay learning time interval. This specifies the amount of time, in seconds, that UNP will delay learning packets received on UNP ports.

`unp delay-learning seconds`

---

**Syntax Definitions**

`seconds` The amount of time to wait before UNP learning starts. The valid range is 0–600 seconds.

---

**Defaults**

By default, the delay learning timer is disabled (timer value is set to 0).

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- To disable the delay learning timer, set the timer value to zero (the default).
- The configured time interval is triggered when the switch boots up. During this time, any packets received on all UNP ports are dropped until the timer expires.
- Configuring a delay learning interval gives the switch time to bring up IP interfaces and for route convergence to complete before any attempt to reach an authentication server is made.

---

**Examples**

```
-> unp delay-learning 250
-> unp delay-learning 600
-> unp delay-learning 0
```

---

**Release History**

Release 8.5R2; command was introduced.
Related Commands

**unp auth-server-down**  Configures a UNP to which a device is classified if MAC or 802.1X authentication fails because the RADIUS server is not reachable.

**show unp global configuration**  Displays the UNP delay learning timer value for the switch.

MIB Objects

alaDaUNPGlobalConfiguration
alaDaUNPDelayLearning
unp auth-server-down

Configures a UNP profile to which a device is classified if authentication fails because the RADIUS server is unreachable.

`unp auth-server-down [voice] {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}`

`no unp auth-server-down [voice] [profile1] [profile2] [profile3]`

---

**Syntax Definitions**

- **profile_name**
  The name of an existing profile to which the device is assigned when the authentication server is unreachable.

- **voice**
  Classifies the IP phone traffic from the data traffic when the authentication server is down.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to remove an authentication server down UNP profile.

- When a device is classified into the specified profile, a configurable authentication down timer is started for that device. When the timer runs out, the authentication process is performed again. If authentication fails again, the device is classified back into the authentication server down profile. The switch will repeat this process until the device authentication is completed.

- Configuring an authentication server down UNP is highly recommended when MAC or 802.1X authentication is enabled on any UNP port or link aggregate. This is because after a switch reload, the traffic from devices connected to UNP ports and link aggregates reaches the switch and triggers the authentication process before route convergence has completed and the server can be reached.
  - If an authentication server down UNP is configured, devices are temporarily learned in that profile and authentication is automatically attempted again after the timeout period expires. This allows time for the server to become reachable from the switch after a reload.
  - If an authentication server down UNP is not configured, devices are learned as filtering and will remain in that state. There is no further attempt to authenticate these devices again.

- If the authentication server down UNP is removed, the authentication server down timer is also removed.
Up to three different profile names are configurable as authentication server down UNP profiles. The profile applied to the traffic is based on the order of precedence and mapping of each profile. For example:

- Profiles mapped to a VLAN are applied only to device traffic received on UNP bridge ports.
- Profiles mapped to a service (SPB, VXLAN, or static) are only applied to device traffic received on UNP access ports.
- When multiple profiles are configured, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the device traffic.

Configuring both a VLAN profile and a service profile ensures that an authentication server down UNP is available for device traffic received on both types of UNP ports (bridge and access).

**Examples**

- `-> unp auth-server-down profile1 unp1-vlan`
- `-> no unp auth-server-down profile1`
- `-> unp auth-server-down profile1 unp1-vlan profile2 unp2-vxlan`
- `-> no unp auth-server-down profile1 profile2`

**Release History**

Release 7.2.1; command was introduced.
Release 7.3.4; command syntax changed; `vxlan-profile` parameter added.
Release 8.3.1; `vlan-profile` and `vxlan-profile` parameters replaced with `profile1`, `profile2`, and `profile3` parameters.
Release 8.5R2; `voice` parameter added.

**Related Commands**

- `unp auth-server-down-timeout` Configures the value for the authentication server down timer.
- `show unp global configuration` Displays the profiles designated as the authentication server down UNP for the switch.

**MIB Objects**

alaDaUNPGlobalConfiguration
alaDaUNPAuthServerDownUnp
unp auth-server-down port-bounce

Configures the port-bounce feature for all authentication server down users globally on all the UNP ports. The port-bounce command forces a re-authentication or a reset of the port when the device gets moved to the new profile.

```
unp auth-server-down port-bounce
no unp auth-server-down port-bounce
```

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
- Use the no form of this command to disable the port-bounce feature for Auth-server-down users.
- The port bounce action only applies to a MAC authenticated non-suppliant (non-802.1x device). If the device is a suppliant (802.1x device), then an EAP-Fail frame is sent instead. In both cases, re-authentication is triggered for both types of devices.

Examples
```
-> unp auth-server-down port-bounce
-> no unp auth-server-down port-bounce
```

Release History
Release 8.5R2; command was introduced.
Related Commands

**show unp global configuration** Displays the profiles designated as the authentication server down UNP for the switch.

MIB Objects

alaDaUNPGlobalConfiguration
  alaDaUNPAuthServerDownPortBounce
**unp auth-server-down-timeout**

Configures the authentication server down timer value. This timer value is applied to devices that are learned in the authentication server down UNP.

`unp auth-server-down-timeout seconds`

`no unp auth-server-down-timeout`

**Syntax Definitions**

`seconds` The number of seconds the authentication server down timer is active. The valid range is 10–43200 seconds.

**Defaults**

By default, the timeout value is set to 60 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to set the timer value back to the default value (60 seconds).
- When this timer expires, devices learned in the authentication server down UNP are cleared from that UNP. The authentication and classification process is attempted again.
- When the authentication server down UNP is removed, the authentication server down timer is also cleared.

**Examples**

```
-> unp auth-server-down-timeout 500
-> unp auth-server-down-timeout 120
-> no unp auth-server-down-timeout
```

**Release History**

Release 7.2.1; command was introduced.
Release 7.3.4; command syntax changed; `vxlan-profile` parameter added.
Release 8.3.1; `vlan-profile` and `vxlan-profile` parameters deprecated.
Release 8.7R3; timeout value range increased to 43200 seconds.
Related Commands

**unp auth-server-down**  
Configures a UNP to which a device is classified if MAC or 802.1X authentication fails because the RADIUS server is not reachable.

**show unp global configuration**  
Displays the authentication server down timeout value for the switch.

MIB Objects

alaDaUNPGlobalConfiguration
  alaDaUNPAuthServerDownTimeout
**unp policy validity-period**

Configures a UNP validity period policy that specifies the days and times during which a device can access the network. This type of policy is assigned to a UNP profile and applied to devices classified into the profile. A device must match all of the policy criteria.

```
unp policy validity-period policy_name [days days] [months months] [hours hh:mm to hh:mm] [interval mm:dd:yy hh:mm to mm:dd:yy hh:mm] [timezone zones]
```

```
no unp policy validity-period policy_name [days days | months months | hours | interval | timezone]
```

---

**Syntax Definitions**

- **policy_name**
  The name of the validity period policy (up to 31 alphanumeric characters).

- **days**
  The day(s) of the week this validity period is active. Enter the actual day of the week (e.g., *monday*, *tuesday*, *wednesday*, etc.).

- **months**
  The month(s) in which the validity period is active. Enter the actual month (e.g., *january*, *february*, *march*, etc.).

- **hh:mm**
  The time of day, specified in hours and minutes, the validity period starts and the time of day the validity period ends (e.g., 10:30 to 11:30).

- **mm:dd:yy hh:mm**
  An interval of time during which the validity period is active. Specify a start and end to the interval period by entering a beginning date and time followed by an end date and time (e.g., 11:01:17 12:01 to 11:02:17 12:01).

- **zones**
  The timezone in which the validity period is active (for example, *pst*, *est*, *gmt*, etc.)
Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>days</td>
<td>no restriction</td>
</tr>
<tr>
<td>months</td>
<td>no restriction</td>
</tr>
<tr>
<td>hh:mm</td>
<td>no specific time</td>
</tr>
<tr>
<td>mm:dd:yyyy hh:mm</td>
<td>no interval</td>
</tr>
<tr>
<td>zones</td>
<td>local timezone</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of the command to remove a UNP period policy from the configuration, or to remove parameters from a particular validity period policy.

- Any combination of the `days`, `months`, `hours`, `interval`, and `timezone` parameters is allowed. The validity period is only in effect when all specified parameters are true.

- Use the `unp profile period-policy` command to associate a period policy with a UNP profile.

Examples

-> unp policy validity-period Office-Time
-> no unp policy validity-period Office-Time

-> unp policy validity-period Office-Time days monday
-> unp policy validity-period Office-Time days monday time-zone IST
-> no unp policy validity-period Office-Time time-zone
-> no unp policy validity-period Office-Time days monday

-> unp policy validity-period Office-Time days all
-> unp policy validity-period Office-Time days all time-zone PST
-> no unp policy validity-period Office-Time days saturday sunday

-> unp policy validity-period Office-Time hours 9:00 to 17:00
-> unp policy validity-period Office-Time hours 9:00 to 17:00 time-zone IST
-> no unp policy validity-period Office-Time hours

-> unp policy validity-period Holiday months december january
-> no unp policy validity-period Holiday months january

-> unp policy validity-period Holiday months december time-zone IST
-> no unp policy validity-period Holiday time-zone
-> no unp policy validity-period Holiday months december

-> unp policy validity-period Seminar interval 02/01/13 10:30 to 02/05/13 16:00
-> no unp policy validity-period Seminar interval

-> unp policy validity-period Seminar interval 02/01/13 10:30 to 02/05/13 16:00
time-zone PST
-> no unp policy validity-period Seminar time-zone
-> no unp policy validity-period Seminar interval

**Release History**

Release 8.1.1; command introduced.

**Related Commands**

- **unp profile period-policy** Assigns a UNP period policy to a profile.
- **show unp policy validity-period** Displays information about the UNP period policy configuration.

**MIB Objects**

alaDaUNFValidityPeriodTable
  - alaDaUNFValidityPeriodName
  - alaDaUNFValidityPeriodDays
  - alaDaUNFValidityPeriodDaysStatus
  - alaDaUNFValidityPeriodMonths
  - alaDaUNFValidityPeriodMonthsStatus
  - alaDaUNFValidityPeriodHour
  - alaDaUNFValidityPeriodHourStatus
  - alaDaUNFValidityPeriodEndHour
  - alaDaUNFValidityPeriodInterval
  - alaDaUNFValidityPeriodIntervalStatus
  - alaDaUNFValidityPeriodEndInterval
  - alaDaUNFValidityPeriodTimezone
  - alaDaUNFValidityPeriodTimezoneStatus
  - alaDaUNFValidityPeriodActiveStatus
unp policy validity-location

Configures a UNP validity location policy that defines a specific location from which a device can access the network. This type of policy is assigned to a UNP profile and applied to devices classified into the profile. A device must match all of the policy criteria defined.

```
unp policy validity-location policy_name [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2] [system-name system_name] [system-location system_location]]
```

```
no unp policy validity-location policy_name [port | linkagg | system-name | system-location]
```

**Syntax Definitions**

- `policy_name` The name of the validity location policy (up to 31 alphanumeric characters).
- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1) of a UNP port. Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number of a UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `system_name` The configured system name for the switch from which the device can access the network.
- `system_location` The configured system location for the switch from which the device can access the network.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>chassis/slot/port[-port2]</code></td>
<td>no restriction</td>
</tr>
<tr>
<td><code>agg_id[-agg_id2]</code></td>
<td>no restriction</td>
</tr>
<tr>
<td><code>system_name</code></td>
<td>no restriction</td>
</tr>
<tr>
<td><code>system_location</code></td>
<td>no restriction</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the `no` form of the command to remove a UNP location policy from the configuration, or to remove parameters from a particular location policy.

- Any combination of the `port`, `linkagg`, `system-name`, and `system-location` parameters is allowed. The location policy is only in effect when all specified parameters are true.

- Use the `unp profile location-policy` command to associate a location policy with a UNP profile.

Examples

```bash
-> unp policy validity-location ALU-NA
-> no unp policy validity-location ALU-NA

-> unp policy validity-location ALU-NA port 1/1/10
-> unp policy validity-location ALU-NA port 1/1/1-5
-> no unp policy validity-location ALU-NA port

-> unp policy validity-location ALU-NA linkagg 10
-> unp policy validity-location ALU-NA linkagg 1-5
-> no unp policy validity-location ALU-NA linkagg

-> unp policy validity-location ALU-NA system-name OS6860
-> no unp policy validity-location ALU-NA system-name OS6860

-> unp policy validity-location ALU-NA system-location US-West
-> no unp policy validity-location ALU-NA system-location
```

Release History

Release 8.1.1; command introduced.

Related Commands

- `unp profile location-policy`: Assigns a UNP location policy to a profile.
- `show unp policy validity-location`: Displays information about the UNP location policy configuration.

MIB Objects

```bash
alaDaUNPLocationPolicyTable
   alaDaUNPLocationPolicyName
   alaDaUNPLocationPolicyPort
   alaDaUNPLocationPolicyPortHigh
   alaDaUNPLocationPolicyPortStatus
   alaDaUNPLocationPolicySystemName
   alaDaUNPLocationPolicySystemLocation
```
**unp domain description**

Configures a customer domain ID to which UNP ports and classification rules are assigned.

```
unp domain domain_id [description domain_description]
no unp domain domain_id description domain_description
```

**Syntax Definitions**

- `domain_id` A numerical customer domain ID.
- `domain_description` An alphanumeric string (1–128 characters).

**Defaults**

By default, customer domain ID zero (0) is assigned to all UNP ports.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_description</td>
<td>Domain ID</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the customer domain ID from the switch configuration. When a domain ID is removed, the following actions are triggered:
  - All UNP ports assigned to that domain are moved to the default domain ID 0.
  - Any classification rules assigned to that domain are removed.
- Customer domains are used to group physical UNP ports or link aggregates into one logical domain.
- Once a port is assigned to a specific customer domain (see the `unp domain` command page), classification rules associated with the same customer domain ID are applied only to UNP ports associated with the same domain ID.

**Examples**

```
-> unp domain 1
-> unp domain 2 description CustomerA
```
Release History

Release 8.3.1; command was introduced.

Related Commands

- **unp domain** Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.
- **show unp domain** Displays the customer domain ID configuration for the switch.

MIB Objects

- alaDaUnpCustomerDomainTable
  - alaDaUnpCustomerDomainId
  - alaDaUnpCustomerDomainDesc
**unp redirect pause-timer**

Configures the global pause timer value for the switch. Use this command to configure the amount of time the switch filters traffic from a non-suppliant (non-802.1X device) on a UNP port. This is done to allow enough time for the switch to clear the authentication state of the non-suppliant, at which time the device is re-authenticated.

```
unp redirect pause-timer seconds
no redirect pause-timer
```

**Syntax Definitions**

`seconds`  
The pause timer value. The valid range is 60–65535

**Defaults**

By default, the pause timer is set to zero.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to reset the pause time back to the default (timer no set).
- The pause timer is triggered when a Change of Authorization (COA) request is received that requires a VLAN change for a non-suppliant (non-802.1X device) and the port bounce action is not triggered for the device.
- During the pause time period, it is expected that the DHCP lease of the client IP in the old VLAN will expire and the client device will re-initiate DHCP resulting in new authentication and a UNP VLAN assignment.
- This command is used when configuring the switch to interact with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch Bring Your Own Devices (BYOD) solution.

**Examples**

```
-> unp redirect pause-timer 180
-> no unp redirect pause-timer
```
**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `unp redirect port-bounce` CONFIGURES the port bounce action for a port or globally for the switch.
- `unp redirect proxy-server-port` CONFIGURES the HTTP proxy port number to use for redirection.
- `unp redirect allowed-name` CONFIGURES a list of additional IP addresses to which a host can access.
- `unp redirect server` CONFIGURES an IP network address to allow HTTP traffic redirection.
- `show unp global configuration` DISPLAYS the global UNP parameter settings for the switch.

**MIB Objects**

- `alaDaUNPGlobalConfiguration`
- `alaDaUNPRedirectPauseTimer`
unp redirect proxy-server-port

Configures the HTTP proxy port number to use for redirection to the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) server.

unp redirect proxy-server-port proxy_port

no unp redirect proxy-server-port

Syntax Definitions

proxy_port The HTTP proxy port number. The valid range is 1024–49151.

Defaults

By default, the redirect proxy port number is set to 8080 (traps HTTP 80, 8080, and 443).

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to set the proxy port number back to the default (8080).
- Configuring the switch to interact with the UPAM or CPPM is done as part of the OmniSwitch implementation of the Bring Your Own Devices (BYOD) solution.

Examples

-> unp redirect proxy-server-port 8887
-> no unp redirect proxy-server-port

Release History

Release 8.1.1; command was introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unp redirect port-bounce</code></td>
<td>Configures the port bounce action for a port or globally for the switch.</td>
</tr>
<tr>
<td><code>unp redirect pause-timer</code></td>
<td>Configures the global pause timer value for the switch.</td>
</tr>
<tr>
<td><code>unp redirect allowed-name</code></td>
<td>Configures a list of additional IP addresses to which a host can access.</td>
</tr>
<tr>
<td><code>unp redirect server</code></td>
<td>Configures an IP network address to allow HTTP traffic redirection.</td>
</tr>
<tr>
<td><code>show unp global configuration</code></td>
<td>Displays the global UNP parameter settings for the switch.</td>
</tr>
</tbody>
</table>

### MIB Objects

- `alaDaUNPGlobalConfiguration`
- `alaDaUNPRedirectServerIP`
**unp redirect server**

Configures an IP network address or a Fully Qualified Domain Name (FQDN) to allow redirection of HTTP traffic to the Unified Policy Access Manager (UPAM) server or the ClearPass Policy Manager (CPPM) server. Specify the address or domain name that is associated with the dynamic URL returned from the UPAM or CPPM server.

```
unp redirect server {ip_address | domain_name}

no unp redirect server
```

**Syntax Definitions**

- `ip_address`: The IPv4 network address (e.g., 171.15.0.0) to which HTTP traffic is redirected.
- `domain_name`: An FQDN (e.g., upam.com) to which HTTP traffic is redirected.

**Defaults**

By default, no redirect server IP address or FQDN is specified.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the redirect server IP or FQDN from the switch configuration.
- If the redirect server IP address or FQDN does not match the UPAM or CPPM server configuration, then redirection to the URL will not work. This provides additional security.
- Configuring the switch to interact with UPAM or CPPM is done as part of the OmniSwitch implementation of the Bring Your Own Devices (BYOD) solution.

**Examples**

```
-> unp redirect server 10.0.0.20
-> no unp redirect server
-> unp redirect server upam.com
-> no unp redirect server
```
**Release History**

Release 8.1.1; command was introduced.
Release 8.5R1; `domain_name` parameter added.

**Related Commands**

- `unp redirect port-bounce` Configures the port bounce action for a port or globally for the switch.
- `unp redirect pause-timer` Configures the global pause timer value for the switch.
- `unp redirect proxy-server-port` Configures the HTTP proxy port number to use for redirection.
- `unp redirect allowed-name` Configures a list of additional IP addresses to which a host can access.
- `show unp global configuration` Displays the global UNP configuration for the switch.

**MIB Objects**

- `alaDaUNPGlobalConfiguration`
- `alaDaUNPRedirectServerIPType`
- `alaDaUNPRedirectServerIP`
**unp redirect allowed-name**

Configures an additional IP subnet to which a host can access. This allows traffic to reach an additional subnet other than that of the Unified Policy Access Manager (UPAM) server or the ClearPass Policy Manager (CPPM) server.

```
unp redirect allowed-name name ip-address ip_address ip-mask ip_mask
no unp redirect allowed-name name
```

**Syntax Definitions**

- **name** Specify a name to assign to the allowed IP network address.
- **ip_address** An IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
- **ip_mask** The IP subnet mask for the allowed IP network address.

**Defaults**

By default, no allowed IP addresses are configured.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove an IP address from the allowed list.
- Explicitly configure and append the allowed IP list to the built-in "restrictedPolicylist" policy list.
- Only one IP subnet can be added.

**Examples**

```
-> unp redirect allowed-name server2 ip-address 10.0.0.20 ip-mask 255.0.0.0
-> no unp redirect allowed-name server2
```

**Release History**

Release 8.1.1; command was introduced.
**Related Commands**

- **unp redirect port-bounce**: Configures the port bounce action for a port or globally for the switch.
- **unp redirect pause-timer**: Configures the global pause timer value for the switch.
- **unp redirect proxy-server-port**: Configures the HTTP proxy port number to use for redirection.
- **unp redirect server**: Configures an IP network address to allow HTTP traffic redirection.
- **show unp global configuration**: Displays the global UNP configuration for the switch.

**MIB Objects**

- `alaDaUNPRedirectAllowedServerTable`
- `alaDaUNPRedirectAllowedServerName`
- `alaDaUNPRedirectAllowedServerIP`
- `alaDaUNPRedirectAllowedMaskIP`
**unp force-l3-learning**

Configures the status of UNP Layer 3 learning on the specified UNP port or globally on all UNP ports. When this functionality is enabled and IP-based classification rules are configured on the switch, only Layer 3 packets are used to learn devices connected to UNP ports. Layer 2 packets are not used for learning devices.

```
unp [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] force-l3-learning [port-bounce]
```

```
no unp [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] force-l3-learning [port-bounce]
```

**Syntax Definitions**

- `chassis/slot/port[-port2]` The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number for a specific UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `port-bounce` Resets the context in which the user device is learned after the device is re-classified with a new IP address. This option is not supported on UNP link aggregates.

**Defaults**

By default, UNP Layer 3 learning is disabled and the port bounce action is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- To disable Layer 3 learning for a specific port or link aggregate, use the `no` form of this command with the `port` or `linkagg` parameter. To globally disable Layer 3 learning, use the `no` form of this command without the `port` or `linkagg` parameter.

- When UNP Layer 3 learning is enabled and there is at least one IP-based classification rule configured, the first packet of the following types of packets is used to learn the device:
  - An IP packet with a non-zero source IP address.
  - A valid ARP/GARP request/reply.
  - DHCP packets, even if the source IP address is 0.0.0.0.

  However, the first packet of the following types of packets is *dropped* and not used to learn the device:
  - Layer 2 frames.
  - Invalid ARP/GARP request/reply (one with sender IP address 0.0.0.0 or 169.254.0.0/16).
- IP packet with a source IP address of 0.0.0.0, except for DHCP packets where the source IP address is 0.0.0.0.

- When Layer 3 learning is enabled and a device is learned and assigned to a UNP profile, any subsequent change to the IP address for that device (for example, the device is assigned a leased IP address) will trigger UNP to re-classify the device based on the new IP address.

- When Layer 3 learning is enforced, the following users learned on a UNP port or link aggregate would not undergo IP reclassification:
  - 802.1x (supplicant) and MAC authenticated (non-supplicant).
  - Users learned through a non-IP-based classification rule that has a higher precedence over IP-based classification rules (such as any UNP extended classification rule, binding rule, MAC address rule, or MAC address range rule).

- When Layer 3 learning is enforced, the following users learned on a UNP port or link aggregate might undergo IP reclassification:
  - Users learned through a non-IP-based classification rule that has a lower precedence than IP-based classification rules (such as a VLAN rule).
  - IP-based classification rule.

- If the port bounce action is enabled for Layer 3 learning, IP reclassification for a user might result in obtaining a new UNP profile based on an IP-based classification rule, and the new UNP profile may assign a VLAN that is different from the initial UNP profile VLAN. If this occurs, the port would be toggled causing the user context to get flushed, and the subsequent packet from the user would then be used to relearn the user. It is assumed that user in this case would subsequently send either a valid ARP packet or an IP packet with a valid source IP address as the first packet, which would be used for re-learning the user directly into the final UNP profile.

- Note that the IP address update/change for an already learned UNP user can happen only when a valid ARP packet is sent from the user after the user is initially learned. As a result, Layer 3 enforcement relies on an ARP packet from the user.

- Whenever an additional port is configured as a UNP port, the Layer 3 learning status is derived from the global setting for the switch.

- When Layer 3 learning is changed at the global level, all port-level configurations are also changed unless a custom port template that configures this function is assigned to the port. For example, when Layer 3 learning is globally disabled, it is automatically disabled on any port that has Layer 3 learning enabled. However, if a port is assigned to a custom port template that enables this function, then the Layer 3 learning status for that port is not changed.

- The port-level setting of the Layer 3 learning function overrides the global setting for the switch. For example, if Layer 3 learning is globally disabled but enabled on port 1/1/20, then Layer 3 learning is active only on port 1/1/20.

Examples

- `unp force-l3-learning`
- `unp force-l3-learning port-bounce`
- `no unp force-l3-learning port-bounce`
- `no unp force-l3-learning`

- `unp port 1/1/20 force-l3-learning`
- `unp port 1/1/20 force-l3-learning port-bounce`
- `no unp port 1/1/20 force-l3-learning port-bounce`
- `no unp port 1/1/20 force-l3-learning`
**Release History**

Release 8.3.1; command was introduced.
Release 8.3.1.R02; `port`, `linkagg`, and `port-bounce` parameters added.

**Related Commands**

- `show unp global configuration` Displays the status of UNP Layer 3 learning for the switch.
- `show unp port config` Displays the status of port-level UNP Layer 3 learning.

**MIB Objects**

alaDaUNPGlobalConfiguration
- alaDaUNPForceL3Learning
- alaDaUNPForceL3LearningPortBounce
alaDaUNPPortTable
- alaDaUNPPortForceL3Learning
- alaDaUNPPortForceL3LearningPortBounce
unp 802.1x-pass-through

Configures the global status of 802.1x pass through for the switch. When this functionality is enabled, 802.1x packets from supplicants attempting to authenticate are not processed on the local switch. Instead, the packets are passed along to another switch for authentication.

unp 802.1x-pass-through

no unp 802.1x-pass-through

Syntax Definitions

N/A

Defaults

By default, 802.1x pass through is disabled for the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to disable 802.1x pass through for the switch.
- Enabling 802.1x pass through on a switch that has an existing UNP or LPS configuration is not recommended. This functionality is intended for a local or intermediate switch when the supplicant device requires authentication through an upstream switch.
- If 802.1x pass through is enabled on a switch that has an existing UNP or LPS configuration, consider the following:
  - 802.1x authentication, 802.1x authentication bypass, and MAC authentication allow EAP functionality is not supported on UNP ports.
  - The initial frame for unknown 802.1x traffic is learned on the switch. If the frame is learned in the forwarding mode, subsequent frames with the same source MAC address are passed through to the next switch. If the frame is learned in the filtering mode, subsequent frames with the same source MAC address are dropped and not passed through.

Examples

- -> unp 802.1x-pass-through
- -> no unp 802.1x-pass-through
Release History

Release 8.4.1.R02; command was introduced.

Related Commands

show unp global configuration  Displays the status of 802.1x pass through for the switch.

MIB Objects

alaDaUNPGlobalConfiguration
alaDaUNP8021XPassThrough
unp ipv6-drop

Configures whether IPv6 packets received on UNP ports are learned or dropped. When this functionality is enabled, IPv6 packets are dropped by UNP on the local switch.

unp ipv6-drop
no unp ipv6-drop

Syntax Definitions

N/A

Defaults

By default, IPv6 packet drop is disabled. IPv6 packets are learned and processed by UNP.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the no form of this command to disable IPv6 packet drop for the switch.

Examples

-> unp ipv6-drop
-> no unp ipv6-drop

Release History

Release 8.5R2; command was introduced.

Related Commands

show unp global configuration Displays the status of IPv6 packet drop for the switch.

MIB Objects

alaDaUNPGlobalConfiguration
alaDaUNPIpv6Drop
unp ap-mode

Configures the global status of the Access Point (AP) mode. The global AP mode status determines the
default AP mode status that is applied when a port or link aggregate is configured as a UNP port. For
example, if the global status is disabled, the port-level status defaults to disabled; if the global status is
enabled, the port-level status defaults to enabled.

unp ap-mode {enable | disable}{secure [enable | disable]}

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Sets the AP mode default status to enabled.</td>
</tr>
<tr>
<td>disable</td>
<td>Sets the AP mode default status to disabled.</td>
</tr>
<tr>
<td>secure</td>
<td>Sets the secure ap-mode configuration.</td>
</tr>
</tbody>
</table>

Defaults

By default, the AP mode is enabled for the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Changing the global AP mode status at any given time is allowed but does not change the port-level
  status set for any existing UNP ports. If the AP mode is disabled for the port, it remains disabled after
  the global status change; if the AP mode is enabled for the port, it remains enabled after the global
  status change and any devices or clients learned on the port are not disrupted.
- To change the AP mode status for a specific UNP port, use the `unp port ap-mode` command.
- Use `secure` parameter to enable or disable the secure ap-mode.

Examples

- -> unp ap-mode disable
- -> unp ap-mode enable
- -> unp ap-mode enable secure enable
- -> unp ap-mode enable secure disable

Release History

Release 8.4.1.R02; command was introduced.
Release 8.8.R1; `secure` parameter added
Related Commands

- **unp port ap-mode** Configures AP mode functionality for a UNP bridge port.
- **show unp global configuration** Displays the status of UNP Layer 3 learning for the switch.

MIB Objects

- alaDaUNPGlobalConfiguration
- alaDaUNPApMode
- alaDaUNPPortApModeSecurity
**unp mac-mobility**

Configures the global status of MAC address mobility; any new UNP service profiles will inherit the global MAC mobility status when the profile is created. Enabling MAC address mobility for a UNP service profile supports VRRP router communication over a Shortest Path Bridging (SPB) service domain.

`unp mac-mobility`

`no unp mac-mobility`

---

**Syntax Definitions**

N/A

**Defaults**

By default, the global MAC address mobility status is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to globally disable UNP MAC address mobility.

- Although the MAC mobility status is configured for UNP profiles, it’s functionality is supported only on profiles mapped to SPB services. SPB service-mapped profiles generate Service Access Points (SAPs) on which a VRRP router can communicate with other VRRP routers across the SPB service domain.

- When a new UNP service profile is created, the MAC mobility status for the profile defaults to the global value. For example, if the global status is enabled, then the new service profile status is set to enabled by default; if the global status is disabled, then the new service profile status is set to disabled by default.

- If the global MAC mobility status is changed at any given time, it will not affect the MAC mobility status of any existing UNP service profiles; the global setting only applies at the time a service profile is created. Any subsequent profiles created will default to the new global MAC mobility status.

- To change the MAC mobility status for a specific UNP service profile, use the `unp profile mac-mobility` command.

**Examples**

```
-> unp mac-mobility
-> no unp mac-mobility
```
**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **unp profile mac-mobility**  
  Configures the MAC mobility status for the specified UNP service profile.

- **show unp global configuration**  
  Displays the status of MAC mobility for the switch.

**MIB Objects**

- alaDaUNPGlobalConfiguration
- alaDaUNPMacMobility
unp user flush

Performs a MAC address flush of Access Guardian users (devices learned on UNP ports) based on the specified port, link aggregate, authentication type, or MAC address.

```
unp user flush [port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]] [sap-id [linkagg] sap_id] [service-id service_id] [authentication-type {mac | 802.1x | none} [profile profile_name] [mac-address mac_address]]
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

- **[linkagg] sap_id**
  - A Service Access Point (SAP) ID. Use the optional `linkagg` parameter if the SAP ID is for a link aggregate.

- **service_id**
  - A service ID.

- **mac**
  - Clears only the MAC authenticated users.

- **802.1x**
  - Clears only the 802.1X authenticated users.

- **none**
  - Clears only the users that have not been authenticated.

- **mac_address**
  - A MAC address (e.g., 00:00:39:59:f1:0c).

- **profile_name**
  - The name of an existing UNP profile.

### Defaults

By default, all MAC addresses learned on all UNP ports are flushed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `port` or `linkagg` parameter to flush users on a specific port or link aggregate.

- Use the `sap-id` parameter to flush users learned on a specific SAP. A SAP ID is comprised of a device-facing port or link aggregate (referred to as a service access port) and an encapsulation value that is used to identify the type of device traffic to map to the associated service.

- Use the `service-id` parameter to flush users learned on a specific service.
Use the **authentication-type** parameter with the **mac**, **802.1x**, or **none** options to flush users that were authenticated (MAC or 802.1X) or users that were not authenticated.

Use the **mac-address** parameter to flush a specific device.

Use the **profile** parameter to flush all users associated with the specified profile name. Combine this parameter with the **mac-address** parameter to flush a specific user associated with the specified profile name.

Combine the **sap-id** or **service-id** parameter with the **profile** parameter option to flush only users on the SAP or service that were classified into the specified profile.

Combine the **sap-id** or **service-id** parameter with the **authentication-type** parameter option to flush only users on the SAP or service that were authenticated with the specified authentication type.

**Examples**

```
-> unp user flush
-> unp user flush port 1/1/6
-> unp user flush linkagg 10
-> unp user flush sap-id 1/1/2:50
-> unp user flush service-id 10
-> unp user flush authentication-type mac
-> unp user flush mac-address 00:11:22:33:44:55
-> unp user flush profile unp1-vlan
-> unp user flush profile unp1-vlan mac-address 00:da:95:11:22:01
```

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

* **show unp user**
  
  Displays information about the devices learned on a UNP port.

**MIB Objects**

```
alaDaUNPUserFlushTable
  alaDaUNPUserFlushIndex
  alaDaUNPUserFlushComplete
  alaDaUNPUserFlushAuthType
  alaDaUNPUserFlushMacAddress
  alaDaUNPUserFlushProfile
  alaDaUNPUserFlushPortStart
  alaDaUNPUserFlushPortEnd
  alaDaUNPUserFlushSapIDIfIndex
  alaDaUNPUserFlushSapIDEncapVal
  alaDaUNPUserFlushServiceID
```
**unp 802.1x eapol-version**

Configures EAPoL version V1 or V3 globally on the switch for 802.1x authentication of users on UNP port.

```
unp 802.1x eapol-version {v1 | v3}
```

### Syntax Definitions

**v1**  
Configures EAPoL version V1 for 802.1x authentication.

**v3**  
Configures EAPoL version V3 for 802.1x authentication.

### Defaults

By default, EAPoL version V1 is configured for 802.1x authentication.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The EAPoL version V3 must be configured on the switch only to authenticate 802.supplicants, which could co-operate with NAS switch using EAPoL version V3.
- When the switch is configured with EAPoL version as V1 or V3, the EAPoL header would carry version 802.1X-2001 (1) or 802.1X-2010 (3) respectively.

### Examples

```
-> unp 802.1x eapol-version v3
```

### Release History

Release 8.7R1; command was introduced.

### Related Commands

- **show unp global configuration**  
  Displays the switch configuration for the global Universal Network Profile (UNP) parameter settings.

### MIB Objects

- **alaDaUNPEapolVersion**
**unp multi-untag-sap**

Enable or disable the multiple untagged user association for UNP dynamic SAP with different services.

```plaintext
unp multi-untag-sap
no unp multi-untag-sap
```

**Syntax Definitions**

N/A

**Defaults**

By default, multiple untagged SAP association is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command allows classification of different untagged users to the same UNP dynamic untagged SAP, which can be associated to different services (like SPB, L2GRE, and VXLAN). For example, MAC-1 on port 1/1/1 gets classified into service with ISID mapping to 1000. Another user MAC-2 on same port 1/1/1 will be allowed to classify into different service with ISID mapping to 2000. This way, SAP 1/1/1:0 would be associated to both ISID 1000 and ISID 2000.
- The untagged SAP creation on different services is supported only for UNP dynamic SAPs.

**Examples**

```
-> unp multi-untag-sap
-> no unp multi-untag-sap
```

**Release History**

Release 8.9R1; command introduced.
**Related Commands**

*show unp global configuration*  Displays the switch configuration for the global Universal Network Profile (UNP) parameter settings.

**MIB Objects**

alaDaUNPMultiUntagSap
**unp profile**

Configures a classification profile that is used to provide role-based access to the switch. This type of profile determines the VLAN or service to which a device can join and applies any additional profile-defined attributes to the device.

When a profile is created with this command, the base command (`unp profile profile_name`) may be used with other command keywords to define attributes for the specified profile. These keywords are listed here and described as separate commands later in this chapter. In addition, some keywords have a `no` form to remove the parameter or return it to its default.

```plaintext
unp profile profile_name
  [qos-policy-list list_name]
  [location-policy policy_name]
  [period-policy policy_name]
  [captive-portal-authentication]
  [captive-portal-profile profile_name]
  [kerberos-authentication]
  [authentication-flag]
  [mobile-tag]
  [maximum ingress-bandwidth bps[k | m]]
  [maximum egress-bandwidth bps[k | m]]
  [maximum ingress-depth bps]
  [maximum egress-depth bps]
  [inactivity-interval seconds]
  [mac-mobility]
  [saa-profile profile_name]

no unp profile profile_name
```

**Syntax Definitions**

- `profile_name`: The name to assign to the UNP classification profile.

**Defaults**

When a profile is created without specifying any parameter values, the profile parameters are set to the following default values:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos-policy-list list_name</td>
<td>No list assigned</td>
</tr>
<tr>
<td>location-policy</td>
<td>No policy assigned</td>
</tr>
<tr>
<td>period-policy</td>
<td>No policy assigned</td>
</tr>
<tr>
<td>captive-portal-authentication</td>
<td>disabled</td>
</tr>
<tr>
<td>captive-portal-profile profile_name</td>
<td>No profile assigned</td>
</tr>
<tr>
<td>kerberos-authentication</td>
<td>disabled</td>
</tr>
<tr>
<td>authentication-flag</td>
<td>disabled</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to remove a profile from the switch configuration.
- Profiles are applied only to traffic received on UNP bridge and access ports or link aggregates.
- After a profile is created, use the `unp profile map` command to map the profile to a VLAN or service.
  - If the profile is mapped to a VLAN, the profile is used to classify traffic received on UNP bridge ports.
  - If the profile is mapped to service parameters, the profile is used to classify traffic received on UNP access ports.
- Any configuration change to a profile will flush all MAC addresses learned on that profile.

Examples

- `-> unp profile unp-profl`
- `-> no unp profile unp-profl`

Release History

Release 8.3.1; command was introduced.
Related Commands

- `unp profile qos-policy-list`: Assigns a QoS policy list to an existing profile.
- `unp profile location-policy`: Assigns a UNP location policy to the specified profile.
- `unp profile period-policy`: Assigns a UNP time-based policy to the specified profile.
- `unp profile captive-portal-authentication`: Configures the status of Captive Portal authentication for the specified profile.
- `unp profile captive-portal-profile`: Assigns a Captive Portal configuration to the specified profile.
- `unp profile kerberos-authentication`: Configures the status of Kerberos snooping for the specified profile.
- `unp profile authentication-flag`: Configures whether the specified profile only allows authenticated devices into the profile.
- `unp profile mobile-tag`: Configures whether a tagged VLAN-port association is created for a device port that is classified into the specified profile.
- `unp profile maximum-ingress-bandwidth`: Configures a maximum ingress bandwidth value that is applied to UNP ports associated with the specified profile.
- `unp profile maximum-egress-bandwidth`: Configures a maximum egress bandwidth value that is applied to UNP ports associated with the specified profile.
- `unp profile maximum-ingress-depth`: Configures a maximum ingress depth value that is applied to UNP ports associated with the specified profile.
- `unp profile maximum-egress-depth`: Configures a maximum egress depth value that is applied to UNP ports associated with the specified profile.
- `unp profile inactivity-interval`: Configures the inactivity interval timer for the specified profile.
- `unp profile mac-mobility`: Configures the MAC address mobility status for the specified UNP service profile to support VRRP router communication over an SPB service domain.
- `unp profile saa-profile`: Assigns an existing Service Assurance Agent (SAA) profile to the specified profile.
- `show unp profile`: Displays the profile configuration for the switch.

MIB Objects

- `alaDaUNPProfileTable`
- `alaDaUNPProfileName`
unp profile qos-policy-list

Configures the QoS policy list attribute for the specified profile. Use this command to assign the name of an existing QoS policy list to the profile. A policy list contains QoS policy rules/ACLs that are applied to devices classified with the associated profile.

unp profile profile_name qos-policy-list list_name

no unp profile profile_name qos-policy-list

Syntax Definitions

profile_name The name of a UNP profile.
list_name The name of a QoS policy list to associate with the specified UNP.

Defaults

By default, no profile attributes are enabled or defined when the profile is created.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the QoS list name from the profile configuration.
- Specifying a QoS policy list name that is inactive or does not already exist in the switch configuration is allowed. However, the list will remain inactive for the UNP until the list is enabled or configured using the QoS policy list command.
- The QoS policy list is used to define the initial role for any UNP user learned in the profile.

Examples

-> unp profile unp-prof1 qos-policy-list unp-list1
-> no unp profile unp-prof1 qos-policy-list unp-list2

Release History

Release 8.3.1; command was introduced.
Related Commands

- **unp profile**
  Configures a UNP classification profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

- **policy list**
  Configures a QoS policy list.

- **show unp profile**
  Displays the profile configuration for the switch.

MIB Objects

- **alaDaUNPProfileTable**
- **alaDaUNPProfileName**
- **alaDaUNPProfileQoSPolicy**
unp profile location-policy

Configures the location policy attribute for the specified profile. Use this command to assign the name of an existing UNP location policy to a profile. This type of policy defines criteria (such as the slot/port, system name and location) to determine if a device is accessing the network from a valid location.

**unp profile** *profile_name* **location-policy** *policy_name*

**no unp profile** *profile_name* **location-policy**

---

**Syntax Definitions**

*profile_name* The name of a UNP profile.

*policy_name* The name of an existing UNP location policy.

---

**Defaults**

By default, no profile attributes are enabled or defined when the profile is created.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the location policy name from the profile configuration.
- The location policy name specified with this command must already exist in the switch configuration.
- Profile location and time period policies are configurable on the switch or on the RADIUS server. If the policies are configured on both the switch and the RADIUS server, then the switch policies take precedence.
- If a UNP device does not meet the criteria applied through the location policy, the device role is changed to unauthorized.

**Examples**

- `-> unp profile unp-prof1 location-policy alu-na`
- `-> no unp profile unp-prof1 location-policy`

**Release History**

Release 8.3.1; command was introduced.
Related Commands

**unp profile**  
Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

**unp policy validity-location**  
Configures a UNP location policy.

**show unp profile**  
Displays the profile configuration for the switch.

MIB Objects

alaDaUNPProfileTable
  alaDaUNPProfileName
  alaDaUNPProfileLocationPolicy
**unp profile period-policy**

Configures the period policy attribute for the specified profile. Use this command to assign the name of an existing UNP period policy to a profile. This type of policy specifies the days and times during which a device can access the network.

```
unp profile profile_name period-policy policy_name
no unp profile profile_name period-policy
```

**Syntax Definitions**

- `profile_name`  
The name of a UNP profile.
- `policy_name`  
The name of an existing UNP period policy.

**Defaults**

By default, no profile attributes are enabled or defined when the profile is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the period policy name from the profile configuration.
- The period policy name specified with this command must already exist in the switch configuration.
- Profile location and time period policies are configurable on the switch or on the RADIUS server. If the policies are configured on both the switch and the RADIUS server, then the switch policies take precedence.
- If a UNP device does not meet the criteria applied through the period policy, the device role is changed to unauthorized.

**Examples**

```
-> unp profile unp-prof1 period-policy office-time
-> no unp profile unp-prof1 period-policy
```

**Release History**

Release 8.3.1; command was introduced.
Related Commands

unp profile
Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

unp policy validity-period
Configures a UNP period policy.

show unp profile
Displays the profile configuration for the switch.

MIB Objects

alaDaUNPProfileTable
  alaDaUNPProfileName
  alaDaUNPProfilePeriodPolicy
**unp profile captive-portal-authentication**

Configures the status of Captive Portal (CP) authentication for the specified UNP profile. When enabled, the Captive Portal authentication process is triggered for devices classified into the profile.

```
unp profile profile_name captive-portal-authentication
no unp profile profile_name captive-portal-authentication
```

**Syntax Definitions**

`profile_name`  
The name of a UNP profile.

**Defaults**

By default, Captive Portal authentication is disabled for the profile.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable Captive Portal authentication for the profile configuration.
- When CP authentication is enabled, the UNP user is assigned an implicit CP pre-login role to facilitate the CP authentication process with the configured CP RADIUS server.
- The CP profile associated with the UNP profile defines the CP RADIUS server to use for the CP authentication process. If a CP profile is not associated with the UNP profile, then the server defined in the global CP configuration for the switch is used instead.
- If CP authentication for the device is successful, the user role is automatically changed according to the CP pass policy list returned from the RADIUS server if it is the highest precedence role known for the user.
- If CP authentication for the device fails, the user role will be changed to the last known highest precedence role for the user.
- When successful CP authentication results in assigning the UNP user to a different profile, CP authentication does not need to be enabled for that profile. For example, if the user is initially assigned to a “Guest” profile and successful CP authentication assigns the user to the “Admin” profile, CP authentication must be enabled on the “Guest” profile but does not have to be enabled on the “Admin” profile.
When CP authentication is disabled for the profile, BYOD redirection is automatically made available to devices assigned to the profile. When CP authentication is enabled, CP is enforced and BYOD redirection is not available.

**Examples**

-> unp profile unp-prof1 captive-portal-authentication
-> no unp profile unp-prof1 captive-portal-authentication

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- `unp profile` Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.
- `show unp profile` Displays the profile configuration for the switch.

**MIB Objects**

- `alaDaUNPProfileTable`  
  - `alaDaUNPProfileName`  
  - `alaDaUNPProfileCPortalAuthentication`
unp profile captive-portal-profile

Configures the Captive Portal (CP) profile attribute for the specified profile. Use this command to assign the name of an existing CP profile to a profile. This type of profile defines a CP configuration that is applied to devices when CP authentication is enabled for the profile.

```
unp profile profile_name captive-portal-profile cp_profile_name
```

```
no unp profile profile_name captive-portal-profile
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>The name of a UNP profile.</td>
</tr>
<tr>
<td>cp_profile_name</td>
<td>The name of an existing UNP Captive Portal profile.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, no CP profile is assigned to a profile.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to remove the CP profile name from the profile configuration.
- The CP profile name specified with this command must already exist in the switch configuration.
- The configuration defined in the CP profile overrides the global CP configuration for the switch.

**Examples**

- `-> unp profile unp-prof1 captive-portal-profile cp-prof`
- `-> no unp profile unp-prof1 captive-portal-profile`

**Release History**

Release 8.3.1; command was introduced.
**Related Commands**

- **unp profile**  
  Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

- **captive-portal-profile**  
  Configures a Captive Portal profile.

- **show unp profile**  
  Displays the profile configuration for the switch.

**MIB Objects**

alaDaUNPProfileTable
  - alaDaUNPProfileName
  - alaDaUNPProfileCPortalProfile
**unp profile kerberos-authentication**

Enables or disables Kerberos snooping on UNP profile.

**unp profile profile_name kerberos-authentication**

**no unp profile profile_name kerberos-authentication**

**Syntax Definitions**

*profile_name*  
The name of a UNP profile.

**Defaults**

By default, Kerberos is disabled on UNP profile.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to disable Kerberos snooping on the UNP profile.
- When Kerberos is disabled on the UNP profile, all users learned in that profile are deleted.
- Although the status of Kerberos snooping is configurable for UNP profiles, it’s functionality is supported only on profiles mapped to a VLAN.
- Kerberos is an L3 authentication. It will be available only after successful L2 authentication.
- Kerberos snooping will work only when the switch has at least one Kerberos server IP address configured.

**Examples**

- `-> unp profile pl kerberos-authentication`
- `-> no unp profile pl kerberos-authentication`

**Release History**

Release 8.6R2; command introduced.
Related Commands

- **kerberos inactivity-timer**: Configures the global inactivity timer for Kerberos users.
- **show kerberos configuration**: Displays the Kerberos global configuration.
- **show unp profile**: Displays the profile configuration for the switch.

MIB Objects

- **alaDaUNPProfileTable**
  - **alaDaUNPProfileKerberosAuthentication**
  - **alaDaUNPProfileRowStatus**
**unp profile authentication-flag**

Configures the authentication flag status for the specified UNP profile. When enabled, only devices successfully authenticated are classified into the profile.

```
unp profile profile_name authentication-flag
no unp profile profile_name authentication-flag
```

**Syntax Definitions**

`profile_name` The name of a UNP profile.

**Defaults**

By default, the authentication flag is disabled for the profile.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the authentication flag for the profile configuration.

- When the authentication flag is enabled for a profile, devices that did not pass L2 authentication (802.1X or MAC) are not allowed into the profile. However, other configured classification options are applied to such devices to determine the appropriate network access control for that device.

**Examples**

```
-> unp profile unp-prof1 authentication-flag
-> no unp profile unp-prof1 authentication-flag
```

**Release History**

Release 8.3.1; command was introduced.
Related Commands

**unp profile**
Confirms a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

**show unp profile**
Displays the profile configuration for the switch.

MIB Objects

alaDaUNPProfileTable
  alaDaUNPProfileName
  alaDaUNPProfileAuthenticationFlag
**unp profile mobile-tag**

Configures the mobile tag status for the specified UNP profile. When enabled, the first user that is learned on a UNP port and classified into the specified UNP profile will cause the UNP port to be added as a tagged member of the VLAN associated with the profile. If the profile is mapped to a service, a tagged virtual port association is created.

```
unp profile profile_name mobile-tag
no unp profile profile_name mobile-tag
```

**Syntax Definitions**

`profile_name`  
The name of a UNP profile.

**Defaults**

By default, the mobile tag status is disabled for the profile.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C4E/V48C8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C32E/T24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the mobile tag status for the profile configuration.
- When the mobile tag status is disabled for a profile, any user device classified into the profile will remain learned in that profile. In this case, the tagged/untagged VLAN-port association would be determined based on the user traffic which was learned as tagged or untagged, respectively.
- If the device port is already an untagged member of the VLAN associated with the profile, then a tagged association is not created.

**Examples**

```
-> unp profile unp-prof1 mobile-tag
-> no unp profile unp-prof1 mobile-tag
```

**Release History**

Release 8.3.1; command was introduced.
Related Commands

unp profile  Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

show unp profile  Displays the UNP profile configuration for the switch.

MIB Objects

alaDaUNPProfileTable
  alaDaUNPProfileName
  alaDaUNPProfileMobileTag
**unp profile maximum-ingress-bandwidth**

Configures the maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the specified profile.

`unp profile profile_name maximum-ingress-bandwidth bps [k | m]`

`no unp profile profile_name maximum-ingress-bandwidth`

### Syntax Definitions

- `profile_name` The name of a UNP profile.
- `bps[k | m]` The maximum amount of bandwidth, in bits-per-second. The valid range is 0–10485760. The value may be entered as an integer (for example, **10**) or with abbreviated units (for example, **10k, 5m**).

### Defaults

By default, the maximum ingress bandwidth value is not defined for the profile.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the maximum ingress bandwidth value for the specified profile. If a maximum ingress depth value is set for the same profile, then both the maximum ingress bandwidth and depth values must be removed together (on the same command line).

- If the maximum ingress bandwidth value is specified as an integer without an abbreviated unit designation, the value is applied in Kbps by default. For example, if the number **10** is specified, **10K** is the value applied.

- If the maximum ingress bandwidth value is set to zero, then all ingress traffic is allowed on the UNP port.

- The maximum ingress bandwidth, egress bandwidth, and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are not applied to UNP link aggregates that are assigned to the profile.
**Examples**

-> unp profile unp-prof1 maximum-ingress-bandwidth 100
-> unp profile unp-prof1 maximum-ingress-bandwidth 10m
-> no unp profile unp-prof1 maximum-ingress-bandwidth
-> unp profile unp-prof1 maximum-ingress-bandwidth 100
-> unp profile unp-prof1 maximum-ingress-depth 50
-> no unp profile unp-prof1 maximum-ingress-bandwidth maximum-ingress-depth

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp profile**
  Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

- **unp profile maximum-ingress-depth**
  Configures how much the traffic can burst over the maximum ingress bandwidth rate.

- **show unp profile**
  Displays the profile configuration for the switch.

- **show unp port bandwidth**
  Displays the bandwidth parameter values applied to a UNP port or link aggregate.

**MIB Objects**

alaDaUNPProfileTable
  alaDaUNPProfileName
  alaDaUNPProfileMaxIngressBandwidth
unp profile maximum-egress-bandwidth

Configures the maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the specified profile.

unp profile profile_name maximum-egress-bandwidth bps [k | m]
no unp profile profile_name maximum-egress-bandwidth

Syntax Definitions

profile_name

The name of a UNP profile.

bps[k | m]

The maximum amount of bandwidth, in bits-per-second. The valid range is 0–10485760. The value may be entered as an integer (for example, 10) or with abbreviated units (for example, 10k, 5m).

Defaults

By default, the maximum egress bandwidth value is not defined for the profile.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900X9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the maximum egress bandwidth value for the specified profile. If a maximum egress depth value is set for the same profile, then both the maximum egress bandwidth and depth values must be removed together (on the same command line).

- If the maximum egress bandwidth value is specified as an integer without an abbreviated unit designation, the value is applied in Kbps by default. For example, if the number 10 is specified, 10K is the value applied.

- If the maximum egress bandwidth value is set to zero, then all egress traffic is allowed on the UNP port.

- The maximum ingress bandwidth, egress bandwidth, and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are not applied to UNP link aggregates that are assigned to the profile.
**Examples**

`-> unp profile unp-prof1 maximum-egress-bandwidth 100`
`-> unp profile unp-prof1 maximum-egress-bandwidth 10m`
`-> no unp profile unp-prof1 maximum-egress-bandwidth`
`-> unp profile unp-prof1 maximum-egress-bandwidth 100`
`-> unp profile unp-prof1 maximum-egress-depth 50`
`-> no unp profile unp-prof1 maximum-egress-bandwidth maximum-egress-depth`

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unp profile</code></td>
<td>Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.</td>
</tr>
<tr>
<td><code>unp profile maximum-egress-depth</code></td>
<td>Configures how much the traffic can burst over the maximum egress bandwidth rate.</td>
</tr>
<tr>
<td><code>show unp profile</code></td>
<td>Displays the profile configuration for the switch.</td>
</tr>
<tr>
<td><code>show unp port bandwidth</code></td>
<td>Displays the bandwidth parameter values applied to a UNP port or link aggregate.</td>
</tr>
</tbody>
</table>

**MIB Objects**

alaDaUNPProfileTable
- alaDaUNPProfileName
- alaDaUNPProfileMaxEgressBandwidth
unp profile maximum-ingress-depth

Configures the maximum ingress queue depth or bucket size assigned to each port that is associated with the specified UNP profile. The depth value is configured in bytes and is used for traffic metering. The queue depth or bucket size determines the amount of buffers allocated to the UNP port. When the queue or bucket size is reached, the switch starts dropping packets.

`unp profile profile_name maximum-ingress-depth bytes`

`no unp profile profile_name maximum-ingress-depth`

Syntax Definitions

(profile_name) The name of a UNP profile.

(bytes) The maximum ingress depth value in bytes. The valid range is 0–16384.

Defaults

By default, the maximum ingress depth value is determined by dividing the maximum ingress bandwidth value by 25. If the result of this calculation is 0 or 1, then 2K is used as the ingress depth value.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to remove the maximum ingress depth value from the profile.

- The maximum ingress depth value is configured in conjunction with the maximum ingress bandwidth parameter. When the ingress depth value is reached, the switch starts to drop packets.

- Configure the maximum ingress bandwidth rate (`unp profile maximum-ingress-bandwidth`) before attempting to set the maximum ingress depth value.

- The maximum ingress bandwidth and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are not applied to UNP link aggregates that are assigned to the profile.

Examples

- `-> unp profile unp-prof1 maximum-ingress-bandwidth 10`
- `-> unp profile unp-prof1 maximum-ingress-depth 5`
-> no unp profile unp-prof1 maximum-ingress-depth

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unp profile</code></td>
<td>Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.</td>
</tr>
<tr>
<td><code>unp profile maximum-ingress-bandwidth</code></td>
<td>Configures the maximum bandwidth limit allocated for ingress traffic on UNP ports assigned to the specified profile.</td>
</tr>
<tr>
<td><code>show unp profile</code></td>
<td>Displays the profile configuration for the switch.</td>
</tr>
<tr>
<td><code>show unp port bandwidth</code></td>
<td>Displays the bandwidth parameter values applied to a UNP port or link aggregate.</td>
</tr>
</tbody>
</table>

**MIB Objects**

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>alaDaUNPProfileTable</code></td>
<td></td>
</tr>
<tr>
<td><code>alaDaUNPProfileName</code></td>
<td></td>
</tr>
<tr>
<td><code>alaDaUNPProfileMaxIngressDepth</code></td>
<td></td>
</tr>
</tbody>
</table>
**unp profile maximum-egress-depth**

Configures the maximum ingress queue depth or bucket size assigned to each port that is associated with the specified UNP profile. The depth value is configured in bytes and is used for traffic metering. The queue depth or bucket size determines the amount of buffers allocated to the UNP port. When the queue or bucket size is reached, the switch starts dropping packets.

```
unp profile profile_name maximum-egress-depth bytes
no unp profile profile_name maximum-egress-depth
```

**Syntax Definitions**

- **profile_name**: The name of a UNP profile.
- **bytes**: The maximum egress depth value in bytes. The valid range is 0–16384.

**Defaults**

By default, the maximum egress depth value is determined by dividing the maximum ingress bandwidth value by 25. If the result of this calculation is 0 or 1, then 2K is used as the ingress depth value.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the maximum egress depth value from the profile.
- The maximum egress depth value is configured in conjunction with the maximum egress bandwidth parameter. When the egress depth value is reached, the switch starts to drop packets.
- Configure the maximum egress bandwidth rate (unp profile maximum-egress-bandwidth) before attempting to set the maximum egress depth value.
- The maximum egress bandwidth and depth values are applied to the port of a user device that is classified into the specified profile.
  - If multiple user devices are classified into different profiles but learned on the same UNP port, the bandwidth parameter values obtained for the last user learned are applied on the port. Parameter values applied through previously learned users are overwritten.
  - Bandwidth parameter values are not applied to UNP link aggregates that are assigned to the profile.

**Examples**

```
-> unp profile unp-prof1 maximum-egress-bandwidth 10
-> unp profile unp-prof1 maximum-egress-depth 5
```
-> no unp profile unp-prof1 maximum-egress-depth

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp profile**
  Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

- **unp profile maximum-egress-bandwidth**
  Configures the maximum bandwidth limit allocated for egress traffic on UNP ports assigned to the specified UNP profile.

- **show unp profile**
  Displays the profile configuration for the switch.

- **show unp port bandwidth**
  Displays the bandwidth parameter values applied to a UNP port or link aggregate.

**MIB Objects**

- **alaDaUNPPProfileTable**
  - **alaDaUNPPProfileName**
  - **alaDaUNPPProfileMaxEgressDepth**
**unp profile inactivity-interval**

Configures whether or not an authenticated device is automatically logged out of the network after a specific period of inactivity (MAC address for the device has aged out). This timer value applies only to devices learned in the specified profile.

```
unp profile profile_name inactivity-interval seconds
```

**Syntax Definitions**

- `profile_name`: The name of a UNP profile.
- `seconds`: The inactivity timer value. The valid range is 10 to 600 seconds.

**Defaults**

By default, the inactivity interval value is set to 10 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Make sure the configured inactivity interval time is set to a value greater than the MAC address aging time for the switch.
- When a specific time is configured for the inactivity interval timer, the device is not logged out of the network if the MAC address aging time expires before the configured timer value.
- When the inactivity interval time is changed for the profile, the new value does not apply to existing authenticated users until the user is flushed out or when the user is authenticated again.
- If a user undergoes MAC authentication and then secondary Captive Portal authentication, the higher of the two inactivity logout timer values returned is applied to the device.
- An inactivity logout timer value is also configurable through authentication, authorization, and accounting (AAA) commands. The value set through the AAA commands takes precedence over the inactivity interval value set for the UNP.

**Examples**

- `-> unp profile unp-prof1 inactivity-interval 500`
- `-> unp profile unp-prof1 inactivity-interval 10`
**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp profile**  
  Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

- **show unp profile**  
  Displays the profile configuration for the switch.

**MIB Objects**

- **alaDaUNPProfileTable**
  - **alaDaUNPProfileName**
  - **alaDaUNPProfileInactivityInterval**
unp profile mac-mobility

Configures the MAC address mobility status for the specified UNP service profile. Enable MAC address mobility for a UNP service profile to support VRRP router communication over an SPB service domain.

**unp profile profile_name mac-mobility**

**no unp profile profile_name mac-mobility**

**Syntax Definitions**

*profile_name*  
The name of a UNP profile that is mapped to SPB service parameters.

**Defaults**

By default, the MAC mobility status for the SPB service-mapped profile is set to the global MAC mobility status when the profile is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the *no* form of this command to disable the MAC mobility status for the profile configuration.
- When the MAC mobility status is disabled for a profile, VRRP MAC address movement that is required for the VRRP master/slave election process is disrupted. This may cause a VRRP configuration to generate two VRRP masters within the SPB service domain.
- Although the MAC mobility status is configured for UNP profiles, it’s functionality is supported only on profiles mapped to SPB services. SPB service-mapped profiles generate Service Access Points (SAPs) on which a VRRP router can communicate with other VRRP routers across the SPB service domain.
- To support VRRP router communication over an SPB service domain, the following configuration is required before the VRRP routers are configured:
  - Enable MAC address mobility for the SPB service-mapped UNP profile.
  - Assign the service profile to a UNP access port to create a persistent UNP SAP on which a VRRP router will communicate. A persistent SAP does not age out and will ensure an uninterrupted flow of VRRP advertisements between the VRRP master and slave routers.

**Examples**

- `-> unp profile unp-prof1 mac-mobility`
- `-> no unp profile unp-prof1 mac-mobility`
**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **unp mac-mobility**
  Configures the global MAC mobility status for the switch.

- **unp profile**
  Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

- **unp profile map service-type spb**
  Configures the mapping of SPB service parameters to the specified UNP profile. The service parameter values are used to define an SPB SAP on which profile traffic is forwarded.

- **show unp profile**
  Displays the UNP profile configuration for the switch.

**MIB Objects**

- **alaDaUNPProfileTable**
  - **alaDaUNPProfileMacMobility**
**unp profile saa-profile**

Assigns a Service Assurance Agent (SAA) profile to the specified UNP profile. Although an SAA profile can be assigned to a UNP profile with this command, an SAA profile is mainly used by the OmniVista network management application to monitor connections between virtual machines (VMs) in a data center network.

```
unp profile profile_name saa-profile profile_name
```

```
no unp profile profile_name saa-profile
```

**Syntax Definitions**

- **profile profile_name**: The name of a UNP profile.
- **saa-profile profile_name**: The name of the SAA profile to assign to the UNP profile.

**Defaults**

By default, no SAA profile is assigned to a UNP profile.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove an SAA profile assignment from a UNP profile configuration.
- The SAA profile specified with this command must already exist in the switch configuration.

**Examples**

```
-> unp profile unp-prof1 saa-profile saa1
```

```
-> no unp profile unp-prof1 saa-profile
```

**Release History**

Release 8.3.1; command was introduced.
Related Commands

**unp profile**  Configures a UNP profile. This type of profile is applied to traffic learned on UNP ports and link aggregates.

**unp saa-profile**  Configures an SAA profile.

**show unp saa-profile**  Displays the SAA profile configuration for the switch.

**show unp profile**  Displays the profile configuration for the switch.

MIB Objects

alaDaUNPProfileTable
  alaDaUNPProfileName
  alaDaUNPProfileSaaProfile
**unp profile map vlan**

Configures the mapping of a standard VLAN to a UNP profile. When a device is assigned to a profile through authentication or classification, the device and the port on which the device was learned are dynamically assigned to the VLAN that is mapped to the profile.

**unp profile profile_name map vlan vlan_id**

---

**Syntax Definitions**

- `profile_name`: The name of an existing UNP profile.
- `vlan_id`: The VLAN ID number to associate with the specified profile name. Devices assigned to the profile are assigned to the associated VLAN.

---

**Defaults**

By default, no mapping configuration is applied to a profile.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Removing a VLAN mapping configuration requires deleting the entire profile from the switch configuration (`no unp profile profile_name`).
- The VLAN associated with a profile must already exist in the switch configuration, unless one of the following conditions occur:
  - The dynamic VLAN configuration functionality is enabled for the switch.
  - The VLAN mapping to a profile is done when the switch boots up.
- Configuring a new VLAN mapping for a profile will overwrite the existing VLAN mapping for that profile. Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.
- Only one type of profile mapping (VLAN or service) is associated with a profile at any given time.
  - If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.
  - If a profile is mapped to service parameters, then the profile is applied to traffic received on UNP access ports.

---

**Examples**

- `-> unp profile unpl-vlan map vlan 10`
Access Guardian Commands

unp profile map vlan

-> no unp profile unpl-vlan

Release History

Release 8.3.1; command was introduced.

Related Commands

unp profile          Configures a UNP profile.
unp dynamic-vlan-configuration          Configures the global UNP status for dynamic VLAN configuration.
unp profile map service-type spb          Maps SPB parameters to a profile. The parameters are used for creating an SPB service access point (SAP) to forward profile traffic.
unp profile map service-type vxlan          Maps VXLAN parameters to a profile. The parameters are used for creating a VXLAN service access point (SAP) to forward profile traffic.
unp profile map service-type static          Maps an existing SPB or VXLAN service ID to a profile.
show unp profile map          Displays the VLAN or service mapping configuration assigned to a UNP profile.

MIB Objects

alaDaUNPProfileTable
  alaDaUNPProfileName
alaDaUNPProfileMapVlanTable
  alaDaUNPProfileMapVlanVlanID
unp profile map service-type spb

Configures the mapping of Shortest Path Bridging (SPB) parameters to the specified UNP profile. When a device is dynamically assigned to the profile through authentication or classification, an SPB service access point (SAP) is automatically created using the specified profile parameters. Traffic from the device is then forwarded on the SAP.

```
unp profile profile_name map service-type spb tag-value {0 | ALL | outer_qtag:all | qtag | outer_qtag:inner_qtag} isid instance_id bvlan bvlan_id [multicast-mode {headend | tandem}] [vlan-translation] [igmp-snooping [profile {default | ipms_profile}]] [mld-snooping [profile {default | ipms_profile}]] [remove-ingress-tag]
```

```
no unp profile profile_name map service-type spb [vlan-translation] [igmp-snooping [profile]] [mld-snooping [profile]] [remove-ingress-tag]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th><strong>profile_name</strong></th>
<th>The name of an existing UNP profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>0</strong></td>
<td>Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).</td>
</tr>
<tr>
<td><strong>qtag</strong></td>
<td>The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.</td>
</tr>
<tr>
<td><strong>outer_qtag:inner_qtag</strong></td>
<td>An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.</td>
</tr>
<tr>
<td><strong>instance_id</strong></td>
<td>A service instance identifier (I-SID) that is used to identify an SPB service in a provider backbone bridge (PBB) network. The valid range is 256–16777214.</td>
</tr>
<tr>
<td><strong>ALL</strong></td>
<td>Any outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.</td>
</tr>
<tr>
<td><strong>outer_qtag:all</strong></td>
<td>An outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.</td>
</tr>
<tr>
<td><strong>bvlan_id</strong></td>
<td>The VLAN ID number of an existing SPB backbone VLAN (BVLAN).</td>
</tr>
<tr>
<td><strong>headend</strong></td>
<td>Specifies the head-end replication mode for the service associated with this UNP.</td>
</tr>
<tr>
<td><strong>tandem</strong></td>
<td>Specifies the tandem replication mode for the service associated with this UNP.</td>
</tr>
<tr>
<td><strong>vlan-translation</strong></td>
<td>Configures egress VLAN translation for the service associated with this UNP.</td>
</tr>
<tr>
<td><strong>igmp-snooping</strong></td>
<td>Configures IGMP snooping for the service associated with this UNP.</td>
</tr>
<tr>
<td><strong>mld-snooping</strong></td>
<td>Configures MLD snooping for the service associated with this UNP.</td>
</tr>
<tr>
<td><strong>ipms_profile_name</strong></td>
<td>The name of an optional IP Multicast Switching profile to use when IGMP or MLD snooping is enabled.</td>
</tr>
<tr>
<td><strong>default</strong></td>
<td>Use default IPMS profile settings for IGMP or MLD snooping.</td>
</tr>
<tr>
<td><strong>remove-ingress-tag</strong></td>
<td>Configures whether or not the customer VLAN tag is removed from ingress packets. Removing the customer VLAN tag is useful when forwarding packets to third-party devices that require untagged packets.</td>
</tr>
</tbody>
</table>
**Defaults**

By default, no mapping configuration is applied to a profile. When the SPB mapping is configured, the following default values are applied for the optional parameters:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast-mode {headend</td>
<td>tandem}</td>
</tr>
<tr>
<td>vlan-xlation</td>
<td>disabled</td>
</tr>
<tr>
<td>igmp-snooping</td>
<td>disabled</td>
</tr>
<tr>
<td>mld-snooping</td>
<td>disabled</td>
</tr>
<tr>
<td>default</td>
<td>ipms_profile_name</td>
</tr>
<tr>
<td>remove-ingress-tag</td>
<td>disabled</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable VLAN translation, IGMP snooping, MLD snooping, or removing the ingress tag for the UNP service profile. To remove any other SPB mapping parameter requires deleting the entire profile from the switch configuration (`no unp profile profile_name`).

- Configuring a new SPB mapping for a profile will overwrite the existing SPB mapping for that profile.

- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.

- Only one type of profile mapping (VLAN or service) is associated with a profile at any given time.
  - If a profile is mapped to service parameters, then the profile is applied to traffic received on UNP access ports.
  - If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.

- The `tag-value` parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the SPB service that is dynamically created based on the specified I-SID and BVLAN values.

- Consider the following when configuring the profile tag value:
  - If the tag value is set to zero, the SAP for the classified traffic is created using the VLAN tags of the traffic. For example, a SAP with an encapsulation value set to 1/12:5 is created when classified traffic received on port 1/12 is single-tagged with VLAN ID 5.
  - Enabling the trust VLAN tag option for the UNP service port triggers the same functionality as setting the service profile tag value to zero. In both cases, the VLAN tags of the classified traffic are used to specify the encapsulation value of the SAP to which the traffic is mapped.
If the trust VLAN tag option is disabled for the UNP port and the service profile tag value is not set to zero (for example, `tag-value 10`), the VLAN tag values of the classified traffic are compared to the configured profile tag value. If the traffic tag values match the profile tag value, the traffic is mapped to the appropriate SAP. If the traffic tags do not match, traffic is not mapped to a SAP.

- If the trust VLAN tag option is disabled for the UNP port and the service profile tag value is not set to zero (for example, `tag-value 10`), the VLAN tag values of the classified traffic are compared to the configured profile tag value. If the traffic tag values match the profile tag value, the traffic is mapped to the appropriate SAP. If the traffic tags do not match, traffic is not mapped to a SAP.

- UNP first checks the switch configuration to see if a SAP already exists for the expected VLAN tag value (CVLAN tags) and I-SID. If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one for the profile traffic.

- If the I-SID specified with this command does not exist in the switch configuration, the switch will dynamically create the expected service and then the SAP as needed.

- The BVLAN ID specified with this command must already exist in the switch configuration.

- Dynamically creating services and related SAPs is subject to available switch resources. If an attempt to dynamically create a service or SAP fails, the MAC addresses classified for the service profile are learned as filtering.

- When an SPB service is configured to use the head-end multicast mode, a non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address.

- When an SPB service is configured to use the tandem multicast mode, a non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address.

- Enabling VLAN translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled. The exception to this is on an OmniSwitch 9900, where VLAN translation is configured only at the service level.

- When configuring the IGMP and MLD snooping mapping parameters, it is necessary to also configure the VLAN translation and multicast mode status for the profile mapping.

**Examples**

```
-> unp profile unp1-spb map service-type spb tag-value 10 isid 1510 bvlan 4001
-> unp profile unp2-spb map service-type spb tag-value 20 isid 1520 bvlan 4002
  multicast-mode tandem vlan-xlation remove-ingress-tag
-> unp profile unp3-spb map service-type spb tag-value 30 isid 1530 bvlan 4003
  vlan-xlation multicast-mode headend igmp-snooping mld-snooping
-> unp profile unp4-spb map service-type spb tag-value 40 isid 1540 bvlan 4004
  vlan-xlation multicast-mode headend igmp-snooping profile ipms-prof1
-> unp profile unp4-spb map service-type spb tag-value 40 isid 1540 bvlan 4004
  vlan-xlation multicast-mode headend mld-snooping profile default

-> no unp profile unp1-spb
-> no unp profile unp2-spb map service-type spb vlan-xlation
-> no unp profile unp2-spb map service-type spb remove-ingress-tag
-> no unp profile unp3-spb map service-type igmp-snooping
-> no unp profile unp3-spb map service-type mld-snooping
-> no unp profile unp4-spb map service-type mld-snooping profile
-> no unp profile unp4-spb map service-type mld-snooping
```

**Release History**

Release 8.3.1; command was introduced.
Release 8.6R1; `igmp-snooping` and `mld-snooping` parameters added.
Release 8.7R2; `remove-ingress-tag` parameter added.
Release 8.8.R1; `ALL` and `outer_qtag:all` parameters added.
Related Commands

- **unp profile**: Configures a UNP profile.
- **unp profile map vlan**: Maps VLAN IDs to a UNP profile. Traffic assigned to the profile is forwarded on the associated VLAN IDs.
- **unp profile map service-type vxlan**: Maps VXLAN parameters to a profile. The parameters are used for creating a VXLAN service access point (SAP) to forward profile traffic.
- **unp profile map service-type static**: Maps an existing SPB or VXLAN service ID to a profile.
- **show unp profile map**: Displays the VLAN or service mapping configuration for the profile.

MIB Objects

- **alaDaUNPProfileTable**
  - **alaDaUNPProfileName**
- **alaDaUNPProfileMapSpbTable**
  - **alaDaUNPProfileMapSpbEncapVal**
  - **alaDaUNPProfileMapSpbIsid**
  - **alaDaUNPProfileMapSpbBVlan**
  - **alaDaUNPProfileMapSpbMulticastMode**
  - **alaDaUNPProfileMapSpbVlanXlation**
  - **alaDaUNPProfileMapSpbIgmpSnooping**
  - **alaDaUNPProfileMapSpbIgmpProfile**
  - **alaDaUNPProfileMapSpbMldSnooping**
  - **alaDaUNPProfileMapSpbMldProfile**
  - **alaDaUNPProfileMapSpbRemoveIngressTag**
unp profile map service-type vxlan

Configures the mapping of Virtual eXtensible LAN (VXLAN) parameters to the specified UNP profile. When a device is dynamically assigned to the profile through authentication or classification, a VXLAN service access point (SAP) is automatically created using the specified profile parameters. Traffic from the device is then forwarded on the SAP.

unp profile profile_name map service-type vxlan tag-value {0 | ALL | outer_qtag:all | qtag | outer_qtag:inner_qtag} vnid vxlan_id {far-end-ip-list ip_list_name [multicast-group mc_group_address] | multicast-group mc_group_address [far-end-ip-list ip_list_name]} [multicast-mode {tandem | headend | hybrid}] [vlan-xlation] [mac-orchestration] [remove-ingress-tag]

no unp profile profile_name map service-type vxlan [far-end-ip-list | multicast-group] [vlan-xlation] [mac-orchestration] [remove-ingress-tag]

Syntax Definitions

profile_name The name of an existing UNP profile.
0 Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
qtag The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.
outer_qtag:inner_qtag An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
ALL Any outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
outer_qtag:all An outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
vxlan_id The VXLAN network identifier that identifies the VLAN segment form where the frames originate. This value is used to create the VXLAN service that is required to dynamically create the SAP.
ip_list_name The name of an existing list that contains the IP addresses for the far-end VXLAN Tunnel End Points (VTEPs). The valid range is 1–32 characters. The IP addresses in this list are used to dynamically create service distribution points (SDPs) for the VXLAN service.
mc_group_address The multicast IP address of the group to which this service will join.
tandem Specifies the tandem replication mode for the service associated with this UNP. This mode uses PIM routing and sends traffic through multicast SDPs.
headend Specifies the head-end replication mode for the service associated with this UNP. This mode sends traffic through unicast SDPs.
hybrid Specifies the hybrid replication mode for the service associated with this UNP. This mode uses both the head-end and tandem methods.
vlan-translation Configures egress VLAN translation for the VXLAN service associated with this UNP.
mac-orchestration
This parameter is automatically configured through OmniSwitch integration with Open vSwitch Database (OVSD) protocols. See the "Web Services, CLI Scripting, OpenFlow, and AOS Micro Services (AMS)" chapter in the OmniSwitch AOS Release 8 Switch Management Guide for more information.

remove-ingress-tag
Configures whether or not the customer VLAN tag is removed from ingress packets. Removing the customer VLAN tag is useful when forwarding packets to third-party devices that require untagged packets.

Defaults
By default, no mapping configuration is applied to a profile. When the VXLAN mapping is configured, the following default values are applied for the optional parameters:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast-mode {headend</td>
<td>tandem</td>
</tr>
<tr>
<td>vlan-xlation {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>mac-orchestration</td>
<td>disabled</td>
</tr>
<tr>
<td>remove-ingress-tag</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
- Use the no form of this command to disable VLAN translation, remove a far-end IP list, remove a multicast group IP address, or disable removing the ingress tag for the profile. To remove any other VXLAN mapping parameter requires deleting the entire profile from the switch configuration (no unp profile profile_name).
- Configuring a new VXLAN mapping for a profile will overwrite the existing VXLAN mapping for that profile.
- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.
- Only one type of profile mapping (VLAN or service) is associated with a profile at any given time.
  - If a profile is mapped to service parameters, then the profile is applied to traffic received on UNP access ports.
  - If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.
The `tag-value` parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the VXLAN service that is dynamically created based on the specified VXLAN ID value.

Consider the following when configuring the profile tag value:

- If the tag value is set to zero, the SAP for the classified traffic is created using the VLAN tags of the traffic. For example, a SAP with an encapsulation value set to 1/12:5 is created when classified traffic received on port 1/12 is single-tagged with VLAN ID 5.
- Enabling the trust VLAN tag option for the UNP service port triggers the same functionality as setting the service profile tag value to zero. In both cases, the VLAN tags of the classified traffic are used to specify the encapsulation value of the SAP on which the traffic is forwarded.
- If the trust VLAN tag option is disabled for the UNP port and the service profile tag value is not set to zero (for example, `tag-value 10`), the VLAN tag values of the classified traffic are compared to the configured profile tag value. If the traffic tag values match the profile tag value, the traffic is forwarded on the SAP. If the traffic tags do not match, traffic is not forwarded on the SAP.

UNP first checks the switch configuration to see if a SAP already exists for the expected VLAN tag value (CVLAN tags). If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one based on the profile attributes for the profile traffic.

If the VXLAN ID specified with this command does not exist in the switch configuration, the switch will dynamically create the expected service and then the SAP as needed.

Dynamically creating services and related SAPs is subject to available switch resources. If an attempt to dynamically create a service or SAP fails, the MAC addresses classified for the service profile are learned as filtering.

The same far-end IP list can be used for multiple services that have to reach the same set of far-end VTEPs.

Configuring both a far-end IP list and a multicast group IP address is allowed for the same profile.

The following multicast modes are supported for a VXLAN service:

- **Tandem**: In this mode, PIM multicast routing is required to discover the neighbor nodes and assign membership to VTEP nodes that desire to be in the same multicast group. This also requires the manual configuration of a multicast SDP object to tunnel traffic to the other VTEP nodes that belong to the same multicast group.
- **Headend**: In this mode, unicast SDP objects are manually configured to tunnel traffic to the far-end nodes. In this case, PIM multicast routing is not required. Any BUM traffic is replicated and one copy is sent to each VTEP node as specified by the unicast SDP object.
- **Hybrid**: In this mode, traffic is tunneled from this service instance to both a group of VTEPs that belong to the same multicast group address and to the VTEP nodes that are not associated with the same multicast group address.

Configuring a VXLAN service on an OmniSwitch 6900-V72/C32 or OmniSwitch 6900-X48C6/T48C6 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.

Enabling VLAN translation at the service level is only applicable if the corresponding access ports for the SAPs also have VLAN translation enabled. The exception to this is on an OmniSwitch 9900, where VLAN translation is configured only at the service level.
Examples

-> unp profile unp1-vxlan map service-type vxlan tag-value 10:12 vnid 100 multicast-group 225.1.1.1
-> unp profile unp2-vxlan map service-type vxlan tag-value 15 vnid 200 far-end-ip-list vtep-list1 vlan-xlation
-> unp profile unp3-vxlan map service-type vxlan tag-value 0 vnid 200 far-end-ip-list vtep-list2 multicast-group 225.1.1.2 remove-ingress-tag
-> no unp profile unp3-vxlan map service-type vxlan vlan-xlation far-end-ip-list remove-ingress-tag
-> no unp profile unp2-vxlan

Release History

Release 8.3.1; command was introduced.
Release 8.7R1; mac-orchestration parameter added.
Release 8.7R2; remove-ingress-tag parameter added.
Release 8.8.R1; ALL and outer_qtag:all parameters added.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp profile</td>
<td>Configures a UNP profile.</td>
</tr>
<tr>
<td>unp profile map vlan</td>
<td>Maps VLAN IDs to a UNP profile. Traffic assigned to the profile is forwarded on the associated VLAN IDs.</td>
</tr>
<tr>
<td>unp profile map service-type spb</td>
<td>Maps SPB parameters to a profile. The parameters are used for creating an SPB service access point (SAP) to forward profile traffic.</td>
</tr>
<tr>
<td>unp profile map service-type static</td>
<td>Maps an existing SPB or VXLAN service ID to a profile.</td>
</tr>
<tr>
<td>unp vxlan far-end-ip-list</td>
<td>Configures a list of IP addresses that represent far-end VXLAN nodes.</td>
</tr>
<tr>
<td>show unp profile map</td>
<td>Displays the VLAN or service mapping configuration for the profile.</td>
</tr>
</tbody>
</table>

MIB Objects

alaDaUNPProfileTable
alaDaUNPProfileName
alaDaUNPProfileMapVxlanTable
alaDaUNPProfileMapVxlanEncapVal
alaDaUNPProfileMapVxlanVnid
alaDaUNPProfileMapVxlanFarEndIPLIST
alaDaUNPProfileMapVxlanMulticastIPAddressType
alaDaUNPProfileMapVxlanMulticastIPAddress
alaDaUNPProfileMapVxlanVlanXlation
alaDaUNPProfileMapVxlanMulticastMode
alaDaUNPProfileMapVxlanMacOrchestration
alaDaUNPProfileMapVxlanRemoveIngressTag
unp vxlan far-end-ip-list

Configures a list of IP addresses, each of which is assigned to the Loopback0 interface of a far-end VXLAN node. The list name is assigned to a profile through the mapping of VXLAN service parameters to the profile. This allows multiple far-end nodes to be associated with the service created for the VXLAN Network ID (VNID) specified in the VXLAN profile.

unp vxlan far-end-ip-list ip_list_name ip_address [ip_address]

no unp vxlan far-end-ip-list ip_list_name [ip_address [ip_address]]

Syntax Definitions

<table>
<thead>
<tr>
<th>ip_list_name</th>
<th>The name of the list that contains the IP addresses for the far-end VXLAN Tunnel End Points (VTEP). The valid range is 1–32 characters.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>The IP address of the Loopback0 interface for the far-end VTEP node. The Loopback0 address is required on every VXLAN node that serves as a VTEP. Use a space to specify a list of IP addresses to assign to the list name.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the far-end list from the switch configuration or to remove an individual IP address from the list.
- The reachability of a far-end IP address is not tested. Make sure the addresses are valid before adding them to the list.
- There is no limit to the number of IP addresses that can be assigned to a single list.
- The same far-end IP list can be used for multiple services that have to reach the same set of far-end VTEPs.
- The far-end IP list is used to build service distribution points (SDPs) for VXLAN services.
- When there is any change to the VXLAN profile, all users associated with that profile are flushed.
• Configuring VXLAN service on an OmniSwitch 6900-V72/C32 is supported only when the service is configured to use the head-end multicast mode; tandem mode services are not supported. If the hybrid mode is selected, only the head-end mode is active.

**Examples**

- `unp vxlan far-end-ip-list vtep-list1 10.1.1.1 11.1.1.1 12.1.1.1 13.1.1.1`
- `no unp vxlan far-end-ip-list vtep-list1 10.1.1.1`
- `no unp vxlan far-end-ip-list vtep-list1`

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `unp profile` Configures a UNP profile.
- `unp profile map service-type vxlan` Maps VXLAN parameters, such as a far-end IP list, to a UNP profile.
- `show unp profile` Displays the profile configuration for the switch.
- `show unp vxlan far-end-ip-list` Displays the contents of VXLAN far-end IP address lists.

**MIB Objects**

- `alaDaUNPVxlanFarEndIPAddressListTable`
  - `alaDaUNPVxlanFarEndIPAddressListIPType`
  - `alaDaUNPVxlanFarEndIPAddressListIP`
- `alaDaUNPVxlanFarEndIPListTable`
  - `alaDaUNPVxlanFarEndIPListName`
  - `alaDaUNPVxlanFarEndIPListIPAddressCount`
  - `alaDaUNPVxlanFarEndIPListRemove`
**unp profile map service-type l2gre**

Configures the mapping of a Layer 2 Generic Routing Encapsulation (L2 GRE) tunnel to the specified UNP profile. When a device is dynamically assigned to the profile through authentication or classification, an L2 GRE Service Access Point (SAP) is dynamically created using the specified service parameters. Traffic from the device is then encapsulated and forwarded through an L2 GRE tunnel to a tunnel aggregation switch.

```
unp profile profile_name map service-type l2gre tag-value {0 | ALL | outer_qtag:all | qtag | outer_qtag:inner_qtag} vpnid vpn_id {far-end-ip-list ip_list_name | far-end-ip ip_address} [vlan-xlation] [remove-ingress-tag]
```

```
no unp profile profile_name map service-type l2gre [far-end-ip-list | far-end-ip] [vlan-xlation] [remove-ingress-tag]
```

**Syntax Definitions**

- **profile_name**
  - The name of an existing UNP profile.
- **0**
  - Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
- **qtag**
  - The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.
- **outer_qtag:inner_qtag**
  - An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
- **ALL**
  - Any outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
- **outer_qtag:all**
  - An outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
- **vpn_id**
  - A GRE tunnel Virtual Private Network (VPN) ID. This is a unique value that is used in the header of a GRE encapsulated packet and should be the same at both ends of a Guest Tunnel.
- **ip_list_name**
  - The name of an existing list that contains the IP address of the Loopback0 interface configured on the far-end tunnel aggregation switch. The valid range is 1–32 characters. The IP address in this list is used to dynamically create the L2 GRE tunnel from the edge switch to the tunnel aggregation switch.
- **ip_address**
  - The IP address of the Loopback0 interface configured on the far-end tunnel aggregation switch.
- **vlan-xlation**
  - Configures egress VLAN translation for the service associated with this UNP.
- **remove-ingress-tag**
  - Configures whether or not the customer VLAN tag is removed from ingress packets. Removing the customer VLAN tag is useful when forwarding packets to third-party devices that require untagged packets.
**Defaults**

By default, no mapping configuration is applied to a profile. When the L2 GRE tunnel service mapping is configured, the following default values are applied for the optional parameters:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-xlation</td>
<td>disabled</td>
</tr>
<tr>
<td>remove-ingress-tag</td>
<td>disabled</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to do the following;
  - remove a far-end IP list or a far-end IP address for the profile.
  - disable VLAN translation for the dynamic SAP.
  - disable removing the ingress tag.

- To remove any other L2 GRE mapping parameters requires deleting the entire profile from the switch configuration (**no unp profile profile_name**).

- The **tag-value** parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the L2 GRE tunnel that is dynamically created based on the specified VPN ID value.

- The same far-end IP address can be used for multiple L2 GRE tunnels that have to reach the same far-end tunnel aggregation switch.

- When L2GRE and VXLAN both are configured on a switch, these services must not use the same gateway.

- Configuring a new L2 GRE tunnel mapping for a profile will overwrite the existing tunnel mapping for that profile.

- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.

- Only one type of profile mapping (VLAN or service) is associated with a profile at any given time.

- A UNP L2 GRE profile is applied to users learned on UNP bridge and access ports.
  - Classifying users learned on UNP access ports into an L2 GRE profile is not supported on the OmniSwitch 6560; only users learned on UNP bridge ports are classified.
  - Classifying users learned on UNP bridge ports into an L2 GRE profile is not supported on the OmniSwitch 6900-T20/T40, OmniSwitch 6900-X20/X40, OmniSwitch 6900-V72/C32,
OmniSwitch 6900-X48C6/T48C6/X48C4E/V48C8/C32E, OmniSwitch 6860N; only users learned on UNP access ports are classified. Port-isolation is also not supported on these platforms.

- Only one UNP L2 GRE profile (one L2 GRE service) can be applied to users learned on UNP bridge ports. The exception to this is on an OmniSwitch 6560 where up to eight UNP L2 GRE profiles (eight L2 GRE services) can be applied to users learned on UNP bridge ports.
- Multiple UNP L2 GRE profiles (multiple L2 GRE services) can be applied to users learned on UNP access ports.
- When users are learned on UNP bridge ports and classified into an L2 GRE profile, the VLAN translation status is not applied. VLAN translation only applies to user traffic learned on UNP access ports.
- The mobile tag functionality is supported on UNP L2 GRE profiles and is applied when users learned on UNP access ports are dynamically assigned to the profile; this functionality is not supported for users learned on UNP bridge ports. Use the `unp profile mobile-tag` command to configure the mobile tag status for the profile.
- There is no VLAN association with the SAP created for the L2 GRE tunnel, so all traffic egressing on the UNP bridge port will be untagged.

- Make sure that only one SAP is associated with the specified VPN ID for this profile.

- UNP first checks the switch configuration to see if an L2 GRE tunnel SAP already exists for the expected VPN ID. If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one based on the profile attributes for the profile traffic.

- If the GRE tunnel VPN ID specified with this command does not exist in the switch configuration, the switch will dynamically create the expected service and then the SAP as needed.

- Dynamically creating services and related SAPs is subject to available switch resources. If an attempt to dynamically create a service or SAP fails, the MAC addresses classified for the UNP GRE tunnel profile are learned as filtering.

- When a Guest Tunnel is established on an underlying physical port, there can be only one gateway supported on that port for carrying the GRE encapsulated traffic.

- When L2GRE is used to tunnel guest traffic from edge switch to tunnel aggregation switch, configure only one L2GRE service on the edge switch. In other scenarios of L2GRE service, it is advised that the auto-discovery is disabled, and all required services and binds are manually configured.

**Examples**

```
-> unp profile guest-profile map service-type l2gre tag-value 0 vpnid 100 far-end-ip 192.168.10.1
-> unp profile guest-profile map service-type l2gre tag-value 0 vpnid 100 far-end-ip-list l2greEndpoint
-> unp profile guest-profile map service-type l2gre tag-value 0 vpnid 200 far-end-ip 192.168.10.1 vlan-xlation remove-ingress-tag
-> no unp profile guest-profile map service-type l2gre far-end-ip-list
-> no unp profile guest-profile map service-type l2gre vlan-xlation
-> no unp profile guest-profile map service-type l2gre remove-ingress-tag
-> no unp profile guest-profile map service-type l2gre
-> no unp profile guest-profile
```

**Release History**

Release 8.4.1.R02; command was introduced.
Release 8.6R1; `vlan-xlation` parameter added.
Release 8.7R2: **remove-ingress-tag** parameter added.
Release 8.8.R1: **ALL** and **outer_qtag:all** parameters added.

**Related Commands**

- **unp profile**
  Configures a UNP profile.

- **unp profile mobile-tag**
  Configures the mobile tag status for the specified profile.

- **unp l2gre far-end-ip-list**
  Configures a list of IP addresses that represent far-end Guest Tunnel Termination Switch.

- **show unp profile map**
  Displays the VLAN or service mapping configuration for the profile.

**MIB Objects**

alaDaUNPProfileTable
  alaDaUNPProfileName
alaDaUNPProfileMapL2GreTable
  alaDaUNPProfileMapL2GreEncapVal
  alaDaUNPProfileMapL2GreVpnid
  alaDaUNPProfileMapL2GreFarEndIPAddressType
  alaDaUNPProfileMapL2GreFarEndIPAddress
  alaDaUNPProfileMapL2GreFarEndIPList
  alaDaUNPProfileMapL2GreRowStatus
  alaDaUNPProfileMapL2GreVlanXlation
  alaDaUNPProfileMapL2GreRemoveIngressTag
**unp l2gre far-end-ip-list**

Configures an IP address list that contains the IP address of the Loopback0 interface configured on the far-end L2 GRE tunnel aggregation switch. The list name is assigned to a profile through the mapping of L2 GRE tunnel parameters to the profile.

**unp l2gre far-end-ip-list** *ip_list_name ip_address*

**no unp l2gre far-end-ip-list** *ip_list_name [ip_address]*

---

**Syntax Definitions**

- **ip_list_name**
  The name of the list that contains the IP address for the far-end tunnel aggregation switch. The valid range is 1–32 characters.

- **ip_address**
  The IP address of the Loopback0 interface for the far-end tunnel aggregation switch.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the far-end list from the switch configuration or to remove the IP address from the list.
- Only one IP address can be assigned to a single list.
- The reachability of a far-end IP address is not tested. Make sure the IP address is valid before adding the address to the list.
- The same far-end IP list can be used on multiple L2 GRE tunnel access switches that have to reach the same tunnel aggregation switch.
- When L2GRE and VXLAN both are configured on a switch, these services must not use the same gateway.
- The far-end IP list is used to build L2 GRE tunnels to the tunnel aggregation switch.
- When there is any change to the L2 GRE profile associated with the far-end IP list, all users associated with that profile are flushed.
Examples

-> unp l2gre far-end-ip-list l2gre-ip-list 192.168.10.1
-> no unp l2gre far-end-ip-list l2gre-ip-list 192.168.10.1
-> no unp l2gre far-end-ip-list l2gre-ip-list

Release History

Release 8.4.1.R02; command was introduced.

Related Commands

unp profile
    Configures a UNP profile.
unp profile map service-type l2gre
    Maps L2 GRE tunnel parameters, such as a far-end IP list, to a UNP profile.
show unp profile
    Displays the profile configuration for the switch.
show unp l2gre far-end-ip-list
    Displays the contents of a far-end IP address list for an L2 GRE tunnel.

MIB Objects

alaDaUNPL2GreFarEndIPAddressListTable
    alaDaUNPL2GreFarEndIPAddressList IPType
    alaDaUNPL2GreFarEndIPAddressList IP
    alaDaUNPL2GreFarEndIPAddressList RowStatus
alaDaUNPL2GreFarEndIPListTable
    alaDaUNPL2GreFarEndIPList Name
    alaDaUNPL2GreFarEndIPList IPAddress Count
    alaDaUNPL2GreFarEndIPList Remove
unp profile map service-type static

Configures the mapping of an existing Shortest Path Bridging (SPB), Virtual eXtensible LAN (VXLAN), or Layer 2 Generic Routing Encapsulation (L2 GRE) service ID to the specified UNP profile. This type of profile mapping is only valid if the specified SPB, VXLAN, or L2 GRE service is already configured; the switch does not dynamically create the service. The specified service ID is then used to dynamically create a service access point (SAP) based on the specified tag value.

```
unp profile profile_name map service-type static tag-value {0 | ALL | outer_qtag:all | qtag | outer_qtag:inner_qtag |} service-id service_id
```

Syntax Definitions

- `profile_name`: The name of an existing UNP profile.
- `0`: Use VLAN tag information from classified traffic to create the Service Access Point (SAP) for the traffic. If the traffic is untagged, the SAP is created with 0 as the encapsulation value (for example, 1/12:0).
- `qtag`: The outer VLAN ID tag to use when creating a SAP for single-tagged traffic.
- `outer_qtag:inner_qtag`: An outer VLAN ID tag and an inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
- `ALL`: Any outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
- `outer_qtag:all`: An outer VLAN ID tag and any inner VLAN tag to use when creating a SAP for double-tagged (QinQ) classified traffic.
- `service_id`: An existing (statically configured) numerical value that identifies a specific SPB, VXLAN, or L2 GRE service. The valid service ID range is 1–32767. Specifying a VXLAN service ID is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

Defaults

By default, no mapping configuration is applied to a profile.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Removing a static service mapping configuration requires deleting the entire profile from the switch configuration (no unp profile profile_name).
- Configuring a new static service mapping for a profile will overwrite the existing static service mapping for that profile.

- Any change to the mapping configuration of the profile will flush all MAC addresses learned on that profile.

- Only one type of profile mapping (VLAN or service) is associated with a profile at any given time.
  - If a profile is mapped to service parameters, then the profile is applied to traffic received on UNP access ports.
  - If a profile is mapped to a VLAN, then the profile is applied to traffic received on UNP bridge ports.

- The **tag-value** parameter specifies the VLAN tag values that are used to create the SAP to which profile traffic is mapped. The SAP is then bound to the service ID value specified with this command.

- Consider the following when configuring the profile tag value:
  - If the tag value is set to zero, the SAP for the classified traffic is created using the VLAN tags of the traffic. For example, a SAP with an encapsulation value set to 1/12:5 is created when classified traffic received on port 1/12 is single-tagged with VLAN ID 5.
  - Enabling the trust VLAN tag option for the UNP service port triggers the same functionality as setting the service profile tag value to zero. In both cases, the VLAN tags of the classified traffic are used to specify the encapsulation value of the SAP to which the traffic is mapped.
  - If the trust VLAN tag option is disabled for the UNP port and the service profile tag value is not set to zero (for example, **tag-value** 10), the VLAN tag values of the classified traffic are compared to the configured profile tag value. If the traffic tag values match the profile tag value, the traffic is mapped to the appropriate SAP. If the traffic tags do not match, traffic is not mapped to a SAP.

- UNP first checks the switch configuration to see if a SAP already exists for the expected VLAN tag value (CVLAN tags) and service ID. If a SAP already exists, the MAC addresses are learned on that SAP. If the SAP does not exist, the switch dynamically creates one for the profile traffic.

- When there is a MAC flush for all UNP users learned and forwarded on the static service ID:
  - UNP triggers the removal of all dynamic SAPs associated with the service ID.
  - The service ID is not removed because the service was statically created; not dynamically generated through UNP.

- A static service ID cannot be removed until all the UNP users learned and forwarded on that service and associated SAPs are deleted.

**Examples**

- `-> unp profile unpl-static map service-type static tag-value 10 service-id 1`
- `-> unp profile unpl2-static map service-type static tag-value 20 service-id 2`
- `-> no unp profile unpl-static`

**Release History**

Release 8.3.1; command was introduced.
Release 8.8.R1; **ALL** and **outer_qtag:all** parameters added.
**Related Commands**

- **unp profile**
  - Configures a UNP profile.

- **unp profile map vlan**
  - Maps VLAN IDs to a UNP profile. Traffic assigned to the profile is forwarded on the associated VLAN IDs.

- **unp profile map service-type spb**
  - Maps SPB parameters to a profile. The parameters are used for creating an SPB service access point (SAP) to forward profile traffic.

- **unp profile map service-type vxlan**
  - Maps VXLAN parameters to a profile. The parameters are used for creating a VXLAN service access point (SAP) to forward profile traffic.

- **show unp profile map**
  - Displays the VLAN or service mapping configuration for the profile.

**MIB Objects**

- alaDaUNPProfileTable
  - alaDaUNPProfileName

- alaDaUNPProfileMapStaticTable
  - alaDaUNPProfileMapStaticEncapVal
  - alaDaUNPProfileMapStaticServiceID
**unp system-default service-mod**

Specifies the modulo number that the switch will use to dynamically calculate an SPB Service Instance Identifier (I-SID) value or a VXLAN Network Identifier (VNID) value for a System Default profile. System Default profiles are dynamically created to accommodate device traffic received on UNP access ports that is not classified into a user-defined UNP service profile.

**unp system-default service-mod {mod_number | default}**

---

**Syntax Definitions**

- **mod_number**
  - The modulo number to use for calculating an SPB I-SID or VNID value.
  - The valid range is 1–4096.

- **default**
  - Sets the modulo number value back to the default value.

---

**Defaults**

By default, modulo 512 is used for the System Default profile calculation.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- A System Default profile is defined to carry traffic for an SPB service or for a VXLAN service based on the dynamic service setting for the UNP access port on which the traffic is received (see the **unp dynamic-service** command). For example:
  - If the dynamic service value is set to SPB, then the System Default profile is dynamically created with attributes to define an SPB SAP.
  - If the dynamic service value is set to VXLAN, then the System Default profile is dynamically created with attributes to define a VXLAN SAP. A System Default profile for a VXLAN SAP is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

- One of the attributes defined for a System Default profile is an SPB I-SID or VXLAN VNID. This value is dynamically calculated using the base service number, modulo number, VLAN tag of the UNP port traffic, and the UNP port domain value. For example, if the base service number is 10000000, the modulo number is 512, the VLAN tag is 30, and the domain is 10, then the following calculation is used to determine the SPB I-SID or VXLAN VNID number:

  \[10000000 + (10 \times 10000) + (30 \mod 512) = 10100030\]

  Based on the above calculation, “10100030” is the resulting service instance value.
Once the SPB I-SID or VXLAN VNID number is determined, that number is used to derive the System Default profile name. For example:

- The name of an SPB System Default profile is “SystemDefaultISID”, where ISID is the calculated attribute value for the profile. For example, if the calculated I-SID number is 10100030, then the SPB profile “SystemDefault10100030” is created.

- The name of a VXLAN System Default profile is “SystemDefaultVNID”, where VNID is the calculated attribute value for the profile. For example, if the calculated VNID number is 10000100, then the VXLAN profile “SystemDefault10001000” is created.

When the modulo number value is changed, all users learned in System Default profiles are flushed (logged out of the network) and dynamic SAPs created for the profiles are cleared.

**Examples**

-> unp system-default service-mod 800  
-> unp system-default service-mod default

**Release History**

Release 8.5R1; command was introduced.

**Related Commands**

- **unp system-default service-base**: Specifies the base service number that the switch will use to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile.
- **unp system-default multicastmode**: Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
- **unp system-default vlan-translation**: Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
- **unp system-default multicastgroup**: Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.
- **unp system-default far-end-ip-list**: Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.
- **show unp global configuration**: Displays the configurable System Default profile values for the switch.
- **unp dynamic-service**: Configures whether the System Default service profile dynamically creates an SPB SAP or a VXLAN SAP based on the traffic received on the UNP access port.

**MIB Objects**

alaDaUNPGlobalConfiguration  
alaDaUNPServiceModule
unp system-default service-base

Specifies the base service number that the switch will use to dynamically calculate an SPB Service Instance Identifier (I-SID) value or a VXLAN Network Identifier (VNID) value for a System Default profile. System Default profiles are dynamically created to accommodate device traffic received on UNP access ports that is not classified into a user-defined UNP service profile.

```
unp system-default service-base {base_number | default}
```

**Syntax Definitions**

- **base_number**: The base service number to use for calculating an SPB I-SID or VNID value. The valid range is 1–1000000.
- **default**: Sets the base service number value back to the default value.

**Defaults**

By default, base service number 10,000,000 is used for the System Default profile calculation.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A System Default profile is defined to carry traffic for an SPB service or for a VXLAN service based on the dynamic service setting for the UNP access port on which the traffic is received (see the `unp dynamic-service` command). For example:
  - If the dynamic service value is set to SPB, then the System Default profile is dynamically created with attributes to define an SPB SAP.
  - If the dynamic service value is set to VXLAN, then the System Default profile is dynamically created with attributes to define a VXLAN SAP. A System Default profile for a VXLAN SAP is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.
- One of the attributes defined for a System Default profile is an SPB I-SID or VXLAN VNID. This value is dynamically calculated using the base service number, modulo number, VLAN tag of the UNP port traffic, and the UNP port domain value. For example, if the base service number is 10,000,000, the modulo number is 512, the VLAN tag is 30, and the domain is 10, then the following calculation is used to determine the SPB I-SID or VXLAN VNID number:

  \[
  10,000,000 + (10 * 10,000) + (30 \% 512) = 10,100,030
  \]

  Based on the above calculation, “10,100,030” is the resulting service instance value.
Once the SPB I-SID or VXLAN VNID number is determined, that number is used to derive the System Default profile name. For example:

- The name of an SPB System Default profile is “SystemDefaultISID”, where ISID is the calculated attribute value for the profile. For example, if the calculated I-SID number is “10,100,030”, then the SPB profile “SystemDefault10100030” is created.

- The name of a VXLAN System Default profile is “SystemDefaultVNID”, where VNID is the calculated attribute value for the profile. For example, if the calculated VNID number is “10,001,000”, then the VXLAN profile “SystemDefault10001000” is created.

When the base service number value is changed, subsequent System Default profiles are created with the new value while profiles created with the previous base value are retained.

**Examples**

```
-> unp system-default service-base 5000
-> unp system-default service-base default
```

**Release History**

Release 8.5R1; command was introduced.

**Related Commands**

- `unp system-default service-base-mod` Specifies the modulo number that the switch will use to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile.

- `unp system-default multicastmode` Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.

- `unp system-default vlan-translation` Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.

- `unp system-default multicastgroup` Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.

- `unp system-default far-end-ip-list` Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.

- `show unp global configuration` Displays the configurable System Default profile values for the switch.

- `unp dynamic-service` Configures whether the System Default service profile dynamically creates an SPB SAP or a VXLAN SAP based on the traffic received on the UNP access port.

**MIB Objects**

- `alaDaUNPGlobalConfiguration` alaDaUNPServiceBase
unp system-default multicastmode

Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.

unp system-default multicastmode {tandem | headend | hybrid}

Syntax Definitions

tandem
Specifies the tandem replication mode for services dynamically created for System Default profiles.

headend
Specifies the head-end replication mode for services dynamically created for System Default profiles.

hybrid
Specifies the hybrid replication mode for services dynamically created for System Default profiles.

Defaults

By default, System Default profile services are configured to use the head-end mode.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The multicast mode selection specified with this command is a global setting that is applied to all of the dynamic services that are created for System Default profiles.

- The following multicast modes are supported for an SPB service:
  - **Tandem**: In this mode, a non-unicast packet received on an SPB access port is replicated once at each node using the multicast group address.
  - **Headend**: In this mode, a non-unicast packet received on an SPB access port is replicated once for each receiver in the provider backbone bridge (PBB) network using its unicast base MAC (BMAC) address.

- The following multicast modes are supported for a VXLAN service:
  - **Tandem**: In this mode, PIM multicast routing is required to discover the neighbor nodes and assign membership to VTEP nodes that desire to be in the same multicast group. This also requires the manual configuration of a multicast SDP object to tunnel traffic to the other VTEP nodes that belong to the same multicast group.
  - **Headend**: In this mode, unicast SDP objects are manually configured to tunnel traffic to the far-end nodes. In this case, PIM multicast routing is not required. Any BUM traffic is replicated and one copy is sent to each VTEP node as specified by the unicast SDP object.
- **Hybrid**: In this mode, traffic is tunneled from this service instance to both a group of VTEPs that belong to the same multicast group address and to the VTEP nodes that are not associated with the same multicast group address.

- A System Default profile for a dynamic VXLAN service is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

**Examples**

- `unp system-default multicastmode tandem`
- `unp system-default multicastmode headend`
- `unp system-default multicastmode hybrid`

**Release History**

Release 8.5R1; command was introduced.
Release 8.6R2; **hybrid** parameter added.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unp system-default vlan-translation</code></td>
<td>Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.</td>
</tr>
<tr>
<td><code>unp system-default multicastgroup</code></td>
<td>Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.</td>
</tr>
<tr>
<td><code>unp system-default far-end-ip-list</code></td>
<td>Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.</td>
</tr>
<tr>
<td><code>show unp global configuration</code></td>
<td>Displays the configurable System Default profile values for the switch.</td>
</tr>
<tr>
<td><code>show unp profile map</code></td>
<td>Displays the VLAN or service mapping configuration for the profile.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- `alaDaUNPGlobalConfiguration`  
  - `alaDaUNPServiceMulticastMode`
**unp system-default vlan-xlation**

Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.

`unp system-default vlan-translation {enable | disable}

### Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables egress translation of VLAN tags.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables egress translation of VLAN tags.</td>
</tr>
</tbody>
</table>

### Defaults

By default, VLAN translation is enabled for System Default profile services.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The VLAN translation status specified with this command is a global setting that is applied to all of the dynamic services that are created for System Default profiles.

- When VLAN translation is enabled for a service, the VLAN tags for outgoing frames on SAPs associated with that service are processed according to the local SAP configuration (the SAP on which the frames will egress) and not according to the configuration of the SAP on which the frames were received.

- When VLAN translation is disabled, frames simply egress without any modification of the VLAN tags. In other words, the frames are transparently bridged without tag modification.

- A System Default profile for a dynamic VXLAN service is supported only on the OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32.

### Examples

- `-> unp system-default vlan-xlation disable`
- `-> unp system-default vlan-xlation enable`

### Release History

Release 8.5R1; command was introduced.
**Related Commands**

- **unp system-default multicastmode**
  Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.

- **unp system-default multicastgroup**
  Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.

- **unp system-default far-end-ip-list**
  Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.

- **show unp global configuration**
  Displays the configurable System Default profile values for the switch.

- **show unp profile map**
  Displays the VLAN or service mapping configuration for the profile.

**MIB Objects**

- alaDaUNPGlobalConfiguration
- alaDaUNPServiceVlanXlation
**unp system-default multicastgroup**

Specifies a multicast group IP address to associate with dynamic VXLAN services that are created for System Default profiles.

```
unp system-default multicastgroup {mc_group_address | default}
```

**Syntax Definitions**

- `mc_group_address` The multicast IP address of the group to which this service will join.
- `default` Sets the multicast group IP address back to the default value (239.0.0.0).

**Defaults**

By default, a VXLAN service associated with a System Default profile will join the 239.0.0.0 multicast group.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The multicast group IP address specified with this command is a global setting that is applied to all of the dynamic VXLAN services that are created for System Default profiles.

- When a dynamic VXLAN service is created for a System Default profile, the specified multicast group IP address is used to build a VXLAN Service Distribution Point (SDP) tunnel for the VXLAN service traffic. VXLAN nodes that subscribe to the same multicast group will receive traffic through the associated SDP tunnel from all the other VXLAN nodes that belong to the same multicast group.

**Examples**

- `unp system-default multicastgroup 225.1.1.2`
- `unp system-default multicastgroup 239.0.0.0`
- `unp system-default multicastgroup default`

**Release History**

Release 8.5R1; command was introduced.
Related Commands

- `unp system-default multicastmode` Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
- `unp system-default vlan-translation` Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
- `unp system-default far-end-ip-list` Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles.
- `show unp global configuration` Displays the configurable System Default profile values for the switch.
- `show unp profile map` Displays the VLAN or service mapping configuration for the profile.

MIB Objects

`alaDaUNPGlobalConfiguration`  
`alaDaUNPServiceMulticastGroup`
unp system-default far-end-ip-list

Specifies the name of a far-end IP list to associate with dynamic VXLAN services that are created for System Default profiles. The list contains IP addresses assigned to the Loopback0 interfaces of far-end VXLAN nodes. This allows multiple far-end nodes to be associated with the dynamic service created for the VXLAN Network ID (VNID) specified in a VXLAN System Default profile.

`unp system-default far-end-ip-list {ip_list_name | default}`

**Syntax Definitions**

- **ip_list_name**
  - The name of the list that contains the IP addresses for the far-end VXLAN Tunnel End Point (VTEP) nodes. The valid range is 1–32 characters.

- **default**
  - Sets the far-end list name to the default value (no list name is specified).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The far-end IP list name specified with this command is a global setting that is applied to all of the dynamic VXLAN services that are created for System Default profiles.

- When a dynamic VXLAN service is created for a System Default profile, the specified IP address list name is used to build VXLAN Service Distribution Point (SDP) tunnels between the VXLAN nodes. Traffic associated with the dynamic VXLAN service is encapsulated and sent through an SDP tunnel to the destined far-end node.

**Examples**

- `-> unp system-default far-end-ip-list vtep-list1`
- `-> unp system-default far-end-ip-list default`

**Release History**

Release 8.5R1; command was introduced.
Release 8.6R2; **default** parameter added.
**Related Commands**

- `unp system-default multicastmode` Specifies the multicast replication mode configuration to use for dynamic services that are created for System Default profiles.
- `unp system-default vlan-translation` Specifies the VLAN translation configuration to use for dynamic services that are created for System Default profiles.
- `unp system-default multicastgroup` Specifies the multicast group IP address to use for dynamic VXLAN services that are created for System Default profiles.
- `show unp global configuration` Displays the configurable System Default profile values for the switch.
- `show unp profile map` Displays the VLAN or service mapping configuration for the profile.

**MIB Objects**

- `alaDaUNPGlobalConfiguration` alaDaUNPServiceFarEndIpList
**unp saa-profile**

Configures a Service Assurance Agent (SAA) performance monitoring profile. This type of profile is assigned to UNP profiles to specify jitter and latency threshold values for SAA sessions that apply to the assigned UNP profile.

```
unp saa-profile profile_name [jitter-threshold jitter_thresh] [latency-threshold latency_thresh]
```

```
no unp saa-profile profile_name
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>The name to assign to the SAA profile.</td>
</tr>
<tr>
<td>jitter_thresh</td>
<td>The jitter threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.</td>
</tr>
<tr>
<td>latency_thresh</td>
<td>The latency threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>jitter_thresh</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>latency_thresh</td>
<td>0 (disabled)</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the SAA profile from the switch configuration.
- Although SAA profiles can be configured and assigned to a UNP through the CLI, these profiles are mainly used by the OmniVista network management application to trigger SAA sessions that monitor connections between virtual machines (VMs) in a data center network.
- Assigning SAA profiles is supported only with UNP profiles that are assigned to UNP bridge ports. UNP access ports do not support this functionality.

**Examples**

- `-> unp saa-profile unp_saa1 jitter-threshold 100 latency-threshold 500`
- `-> unp saa-profile unp_saa2 jitter-threshold 150`
- `-> unp saa-profile unp_saa3 latency-threshold 250`
**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- `unp profile saa-profile` Assigns an SAA profile to the specified UNP profile.
- `show unp saa-profile` Displays the SAA profile configuration for the switch.
- `show unp profile` Displays the profile configuration for the switch.

**MIB Objects**

alaDaSaaProfileTable
  alaDaSaaProfileName
  alaDaSaaProfileLatencyThreshold
  alaDaSaaProfileJitterThreshold
**unp port-type**

Configures UNP functionality for the specified port or link aggregate. This includes configuring the UNP port type (bridge or access). Traffic received on a UNP bridge port is classified using VLAN profiles and port attributes. Traffic received on a UNP access port is classified using service profiles and port attributes.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id1[-agg_id2]} port-type {access | bridge}
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id1[-agg_id2]}
```

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port1[-port]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id1[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (5-10).
- **access**: Configures the specified port or link aggregate as a service access port. This port type is used for classifying traffic into service-based profiles. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*
- **bridge**: Configures the specified port or link aggregate as a standard bridge port. This port type is used for classifying traffic into VLAN-based profiles.

---

**Defaults**

By default, UNP is disabled on all ports and link aggregates.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to remove the UNP configuration from a port or link aggregate.
- Any configuration change to a UNP-enabled port will flush all MAC addresses learned on that port. This applies only to CLI commands used to configure UNP port parameters.
- Only one UNP port type is configurable for a specific port or link aggregate. To change the port type of an existing UNP port, remove the current UNP configuration first using the **no unp port** or **no unp linkagg** command then use the **unp port-type** command to set the new port type.
- There is no limit to the number of switch ports that can have UNP enabled.
Enabling UNP is not supported on the following switch ports:
- 802.1q-tagged ports.
- MVRP ports.
- Port Mirroring destination ports (MTP).
- Port Mapping network ports.
- STP and ERP ports.
- Ports on which a static MAC address is configured.
- Ports on which dynamic Source Learning is disabled.
- VLAN Stacking (Ethernet Services NNI or UNI) ports.
- Service Manager access and network ports.
- Ethernet OAM ports.

UNP and Learned Port Security (LPS) are supported on the same port with the following conditions:
- LPS is not supported on link aggregates.
- The LPS learning window is set globally but not on a per-port basis. So the window applies to all UNP ports.
- When LPS is enabled or disabled on a UNP bridge port (LPS is not supported on UNP access ports), MAC addresses already learned on that port are flushed.
- Configuring a static MAC address is not allowed on a UNP port unless LPS is also enabled on the same port.
- When both LPS and UNP are enabled on the same port, UNP first authenticates and classifies any MAC addresses received, then LPS rules are applied. If a MAC address violates any of the LPS rules for the port, the address may get filtered or the port violated even if UNP initially determined the address was valid. In other words, LPS rules take precedence over UNP to determine if a MAC address is bridged or filtered on the port.
- If UNP classifies a MAC address as learning but LPS learns the address as filtering, an untagged packet will show as filtering in the default VLAN for the port and a tagged packet MAC will show as filtering in the specific tagged VLAN.
- When a MAC address is filtered by LPS, the show unp user command will display “LPS-Blocked” as the classification source for that MAC address.

UNP ports support both tagged and untagged packets. If the VLAN ID of a tagged packet matches the VLAN associated with a UNP into which the packet was classified, the packet is learned as forwarding and a tagged VLAN-port association is created. However, if the VLAN ID tag does not match the VLAN ID associated with the profile, the packet is filtered.

UNP bridge and access ports support single-tagged and double-tagged packets with the following conditions:
- Double-tagged packets are treated the same as single-tagged packets in that UNP will only use the outer VLAN tag to determine how the packet is processed on the UNP bridge port.
- UNP access ports use the inner VLAN tag of double-tagged packets received on the port to determine the service access port (SAP) to use or create for forwarding the traffic on the network backbone.
Access Guardian Commands

**Examples**

- unp port 1/1 port-type access
- unp port 1/1-3 port-type bridge
- unp port 1/10 port-type access
- no unp port 1/10
- unp linkagg 5 port-type access
- unp linkagg 8 port-type bridge
- unp linkagg 2 port-type access
- no unp linkagg 2

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp admin-state**  
  Configures the administrative status of the UNP configuration for the specified port or link aggregate.

- **unp profile**  
  Configures a UNP profile that is used to classify traffic received on UNP ports.

- **show unp port**  
  Displays the UNP configuration for the port.

**MIB Objects**

- alaDaUNPPortTable
- alaDaUNPPortIfIndex
- alaDaUNPPortType
**unp l2-profile**

Assigns an existing Layer 2 profile to the specified UNP access port. This profile determines how Layer 2 protocol frames received on the access port are processed.

```
unp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} l2-profile l2profile_name
no unp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} l2-profile
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The chassis number and the slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **l2profile_name**
  - The name of an existing Layer 2 profile.

**Defaults**

By default, the Layer 2 profile “unp-def-access-profile” is assigned when a port is configured as a UNP access port.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the Layer 2 profile configuration from the UNP port.

- Specify only ports or link aggregates that are configured as UNP access ports. This command does not apply to UNP bridge ports.

- Specify a Layer 2 profile name that already exists in the switch configuration. Layer 2 profiles are created using the **service l2profile** command.

**Examples**

- `-> unp port 1/1/3 l2-profile sap_1_profile`
- `-> unp linkagg 10 l2-profile sap_1_profile`
- `-> unp port 1/1/3 l2-profile unp-def-access-profile`
- `-> unp linkagg 10 l2-profile unp-def-access-profile`
- `-> no unp port 1/1/3 l2-profile`
- `-> no unp linkagg 10 l2-profile`
**Release History**

Release 8.4.1; command was introduced.

**Related Commands**

- `unp port-type` Configures UNP functionality on a port or link aggregate.
- `service l2profile` Configures a Layer 2 profile that is used to specify how to process Layer 2 control frames ingressing on the access port.
- `show service l2profile` Displays the Layer 2 profile configuration information for the bridge.
- `show unp port config` Displays the UNP configuration for the port.

**MIB Objects**

- `alaDaUNPPortTable`
  - `alaDaUNPPortIfIndex`
  - `alaDaUNPPortL2Profile`
unp redirect port-bounce

Enables or disables the port bounce action on the specified UNP bridge port or globally on all UNP bridge ports. When enabled, a port bounce is triggered upon receipt of a RADIUS Change of Authorization (COA) or a Disconnect request (DM) message from a redirection server to enforce a user role or terminate a user session.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} redirect port-bounce
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} redirect port-bounce
```

```
unp redirect port-bounce {enable | disable}
```

**Syntax Definitions**

- `chassis/slot/port1[-port2]`: The chassis ID, slot, and port number (3/1/1) for a specific UNP bridge port. Use a hyphen to specify a range of ports (3/1/1-8).
- `agg_id[-agg_id2]`: The link aggregate ID number for a specific UNP bridge link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `enable`: Globally enables the port bounce function for all UNP bridge ports.
- `disable`: Globally disables the port bounce function for all UNP bridge ports.

**Defaults**

By default, port bounce is disabled on all UNP bridge ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `port` or `linkagg` parameter to enable port bounce for a specific UNP bridge port or link aggregate. Use the `no` form of this command to disable port bounce for a specific UNP bridge port or link aggregate. Note that port bounce is not supported on UNP access ports.
- Use the `enable` or `disable` parameters to globally enable or disable the port bounce status for all UNP bridge ports or link aggregates on the entire switch.
- The port bounce action only applies to a MAC authenticated non-suppliant (non-802.1X device). If the device is a supplicant (802.1X device), then an EAP-Fail frame is sent instead. In both cases, re-authentication is triggered for both types of devices.
The port-level setting of the port bounce action overrides the global setting for the switch. The following table indicates when a port is toggled based on the status of port bounce at the global and port level:

<table>
<thead>
<tr>
<th>Global Port Bounce</th>
<th>Per-Port Bounce</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>Port is not toggled</td>
</tr>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>Port is toggled</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>Port is toggled</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>Port is not toggled</td>
</tr>
</tbody>
</table>

This command is used when configuring the switch to interact with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch Bring Your Own Devices (BYOD) solution.

**Examples**

Port-level configuration example:

```
-> unp port 1/1/6 redirect port-bounce
-> no unp port 1/1/6 redirect port-bounce
```

Global configuration example:

```
-> unp redirect port-bounce enable
-> unp redirect port-bounce disable
```

**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; no form of this command added for specific port or link aggregate configuration.

**Related Commands**

- `unp port-type` Configures UNP functionality on a port or link aggregate.
- `unp redirect pause-timer` Configures the global pause timer value for the switch
- `unp redirect proxy-server-port` Configures the HTTP proxy port number to use for redirection.
- `unp redirect server` Configures an IP network address to allow HTTP traffic redirection.
- `unp redirect allowed-name` Configures a list of additional IP addresses to which a host can access.
- `show unp port` Displays the UNP configuration for the port.
- `show unp global configuration` Displays the profile designated as the authentication server down UNP for the switch.

**MIB Objects**

- `alaDaUNPPortTable`  
  - `alaDaUNPPortIfIndex`  
  - `alaDaUNPPortRedirectPortBounce`  
- `alaDaUNPGlobalConfiguration`  
  - `alaDaUNPRedirectPortBounce`
**unp 802.1x-authentication**

Configures the status of 802.1X authentication for the specified UNP port. Enable this functionality to invoke 802.1X-based authentication for devices connected to the UNP port.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>chassis</code></td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td><code>slot/port[-port2]</code></td>
<td>The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).</td>
</tr>
<tr>
<td><code>agg_id[-agg_id2]</code></td>
<td>Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).</td>
</tr>
</tbody>
</table>

### Defaults

By default, 802.1X authentication is enabled on UNP ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to disable 802.1X authentication on a UNP port or link aggregate.
- This command is only allowed on UNP-enabled ports and link aggregates.
- If a range of ports or link aggregates is specified with this command, any non-UNP ports or aggregates within the range are skipped.
- An option exists to classify a device into an alternate UNP in the event successful 802.1X authentication does not return a UNP name. See the **unp 802.1x-authentication pass-alternate** command.
- If UNP MAC authentication, 802.1X authentication, and classification (see **unp classification** and **unp mac-authentication**) are disabled on the UNP port, all MAC addresses received on that port are blocked unless a default UNP is configured.
- Configuring an authentication server down UNP (see **unp auth-server-down**) is highly recommended when MAC or 802.1X authentication is enabled on VLAN bridge or SPB access ports or aggregates. This is because after a switch reload, traffic from devices connected to these types of ports and
aggregates reaches the switch and triggers the authentication process before route convergence has completed and the server can be reached.

- If an authentication server down UNP is configured, devices are temporarily learned in that profile and authentication is automatically attempted again after the timeout period expires. This allows time for the server to become reachable from the switch after a reload.
- If an authentication server down UNP is not configured, devices are learned as filtering and will remain in that state. There is no further attempt to authenticate these devices again.
- The authentication server down functionality is not supported on VXLAN access ports or aggregates.

**Examples**

- `unp port 1/1/5 802.1x-authentication`
- `no unp port 1/1/5 802.1x-authentication`

- `unp port 1/1/10-15 802.1x-authentication`
- `no unp port 1/1/10-15 802.1x-authentication`

- `unp linkagg 10 802.1x-authentication`
- `no unp linkagg 10 802.1x-authentication`

- `unp linkagg 10-50 802.1x-authentication`
- `no unp linkagg 10-50 802.1x-authentication`

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `unp port-type` Configures UNP functionality on a port or link aggregate.
- `unp 802.1x-authentication` Assigns the device to another profile when successful 802.1X authentication does not return a UNP name.
- `pass-alternate` Configures the MAC authentication status for the UNP port.
- `unp classification` Configures the classification status for the UNP port.
- `unp auth-server-down` Configures an authentication server down UNP for the switch.
- `show unp port` Displays the UNP configuration for the port.

**MIB Objects**

- `alaDaUNPPortTable` 
  - `alaDaUNPPortIfIndex` 
  - `alaDaUNPPort8021XAuthStatus`
unp 802.1x-authentication pass-alternate

Configures the name of an existing UNP to use as an alternate profile. A device is assigned to the alternate profile when successful 802.1X authentication does not return the name of a profile.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication pass-alternate profile_name

no unp {port chassis/slot/port1[-port2] | linkagg agg_id} 802.1X-authentication pass-alternate
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `profile_name` The name of an existing VLAN, SPB, or VXLAN profile.

**Defaults**

By default, no alternate UNP is configured.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the alternate profile from the UNP port configuration.
- This command is only allowed on UNP-enabled ports and link aggregates.
- If a range of ports or link aggregates is specified with this command, any non-UNP ports or aggregates within the range are skipped.
- The profile name specified with this command must already exist in the switch configuration.

**Examples**

- `unp port 1/1/1 802.1x-authentication pass-alternate Finance`
- `unp port 1/1/1-3 802.1x-authentication pass-alternate CustomerA`
- `no unp port 1/1/1-3 802.1x-authentication pass-alternate`
- `unp linkagg 5 802.1x-authentication pass-alternate AltUNP`
- `unp linkagg 10-15 802.1x-authentication pass-alternate CustomerB`
-> no linkagg 5 mac-authentication pass-alternate

**Release History**

Release 7.3.4; command was introduced.
Release 8.3.1; **vlan-profile**, **spb-profile**, and **vxlans-profile** parameters deprecated.

**Related Commands**

- **unp profile**
  Configures a UNP profile that is used to classify traffic received on UNP ports.

- **unp port-type**
  Configures UNP functionality on a port or link aggregate.

- **unp 802.1x-authentication**
  Configures the 802.1X authentication status for the UNP port.

- **show unp port**
  Displays the UNP port parameter configuration.

**MIB Objects**

- **alaDaUNPPortTable**
  - **alaDaUNPPortIfIndex**
  - **alaDaUNPPort8021XPassAltProfileName**
unp 802.1x-authentication tx-period

Configures the 802.1X authentication re-transmission time interval for the specified UNP port.

`unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication tx-period seconds`

`no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication tx-period`

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
- **seconds**: The amount of time before an EAP Request Identity is retransmitted. The valid range is 1–60 seconds.

**Defaults**

By default, the retransmission period is set to 30 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to set the re-transmission time interval back to the default value of 30 seconds.
- The re-transmission time period only applies to UNP ports on which 802.1X authentication is enabled.
- If a range of ports is specified with this command, any non-UNP ports within the range are skipped.

**Examples**

- `unp port 1/1/5 802.1x-authentication tx-period 60`
- `no unp port 1/1/6-10 802.1x-authentication tx-period 20`
- `unp linkagg 10 802.1x-authentication tx-period 60`
- `no unp linkagg 20-25 802.1x-authentication tx-period`
Release History

Release 7.3.4; command was introduced.

Related Commands

- `unp port-type` Configures UNP functionality on a port or link aggregate.
- `unp 802.1x-authentication` Configures the 802.1X authentication status for the UNP port.
- `show unp port` Displays the UNP configuration for the port.

MIB Objects

- `alaDaUNPPortTable` Configures the 802.1X authentication status for the UNP port.
- `alaDaUNPPort8021XTxPeriod` Displays the UNP configuration for the port.
**unp 802.1x-authentication supp-timeout**

Configures the 802.1X authentication supplicant timeout for the specified UNP port. This value is the amount of time the switch will wait before timing out an 802.1X user that is attempting to authenticate.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication supp-timeout seconds
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication supp-timeout
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port1[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15)
- `seconds` The timeout value. The valid range is 1–120 seconds.

**Defaults**

By default, the supplicant timeout value is set to 30 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to set the supplicant timeout back to the default value of 30 seconds.
- Increase the supplicant timeout value if the authentication process requires additional steps by the user (for example, entering a challenge).
- The supplicant timeout is applied only to 802.1X users connected to a UNP port on which 802.1X authentication is enabled.
- If a range of ports is specified with this command, any non-UNP ports within the range are skipped.

**Examples**

```
-> unp port 1/1/5 802.1x-authentication supp-timeout 10
-> unp port 1/1/10-15 802.1x-authentication supp-timeout 60
-> no unp port 1/1/5 802.1x-authentication supp-timeout
```
-> unp linkagg 10 802.1x-authentication supp-timeout 40
-> unp linkagg 2-5 802.1x-authentication supp-timeout 40
-> no unp linkagg 10 802.1x-authentication supp-timeout

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- **unp port-type**: Configures UNP functionality on a port or link aggregate.
- **unp 802.1x-authentication**: Configures the 802.1X authentication status for the UNP port.
- **show unp port**: Displays the UNP configuration for the port.

**MIB Objects**

- **alaDaUNPPortTable**
  - **alaDaUNPPort8021XSuppTimeOut**
**unp 802.1x-authentication max-req**

Configures the maximum number of times the switch will retransmit a request for authentication information (request identity, password, challenge) to an 802.1X user on the specified UNP port.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication max-req max_req
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication max-req
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

- **max_req**
  - The maximum number of times information requests are retransmitted. The valid range is 1–3.

**Defaults**

By default, the maximum number of requests is set to two.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>X48C6E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to set the maximum number of times information requests are retransmitted back to the default value of two.

- The 802.1X requests are transmitted, up to the maximum number allowed, until the authentication session is shut down based on the supplicant timeout value configured for the 802.1X port.

- The maximum number of requests is applied only to 802.1X users connected to a UNP port on which 802.1X authentication is enabled.

- If a range of ports or link aggregates is specified with this command, any non-UNP ports within the range are skipped.

**Examples**

```
-> unp port 1/1/5 802.1x-authentication max-req 10
```
-> unp port 1/1/10-15 802.1x-authentication max-req 5
-> no unp port 1/1/5 802.1x-authentication max-req
-> unp linkagg 10 802.1x-authentication max-req 10
-> unp linkagg 2-5 802.1x-authentication max-req 5
-> no unp linkagg 10 802.1x-authentication max-req

Release History
Release 7.3.4; command was introduced.

Related Commands

unp 802.1x-authentication supp-timeout
Configures the number of seconds before the switch will time out an 802.1X user that is attempting to authenticate.

unp port-type
Configures UNP functionality on a port or link aggregate.

unp 802.1x-authentication
Configures the 802.1X authentication status for the UNP port.

show unp port
Displays the UNP configuration for the port.

MIB Objects
alaDaUNPPortTable

alaDaUNPPort8021XMaxReq
**unp 802.1x-authentication bypass-8021x**

Configures whether the 802.1X authentication process is bypassed on the specified UNP port. When enabled, the 802.1X device authentication process is skipped; only MAC authentication or rule-based classification is applied to device traffic on the UNP port.

```
unp {port chassis/slot/port1 [-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication bypass-8021x
```

```
no unp {port chassis/slot/port1 [-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication bypass-8021x
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

**Defaults**

By default, 801.1X authentication bypass is disabled on the UNP port; 802.1X authentication is attempted first.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is only allowed on UNP-enabled ports and link aggregates.
- Enabling 802.1X authentication bypass is not allowed on UNP ports that are configured with an 802.1X authentication failure policy.

**Examples**

```
-> unp port 1/1/5 802.1x-authentication bypass-8021x
-> no unp port 1/1/5 802.1x-authentication bypass-8021x
-> unp port 1/1/10-15 802.1x-authentication bypass-8021x
-> no unp port 1/1/10-15 802.1x-authentication bypass-8021x
```

```
-> unp linkagg 10 802.1x-authentication bypass-8021x
-> no unp linkagg 10 802.1x-authentication bypass-8021x
-> unp linkagg 2-5 802.1x-authentication bypass-8021x
-> no unp linkagg 2-5 802.1x-authentication bypass-8021x
```
**Release History**
Release 7.3.4; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp port-type</td>
<td>Configures UNP functionality on a port or link aggregate.</td>
</tr>
<tr>
<td>unp 802.1x-authentication</td>
<td>Configures the 802.1X authentication status for the UNP port.</td>
</tr>
<tr>
<td>unp mac-authentication allow-eap</td>
<td>Configures whether or not subsequent 802.1X authentication is attempted based on the MAC authentication results.</td>
</tr>
<tr>
<td>show unp port</td>
<td>Displays the UNP configuration for the port.</td>
</tr>
</tbody>
</table>

**MIB Objects**

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaDaUNPPortTable</td>
<td></td>
</tr>
<tr>
<td>alaDaUNPPort8021XBypassStatus</td>
<td></td>
</tr>
</tbody>
</table>
**unp 802.1x-authentication failure-policy**

Configures whether the switch attempts subsequent MAC authentication for a device after the initial 802.1X authentication process fails.

**Syntax**

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication failure-policy {mac}
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x-authentication failure-policy
```

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port[-port2]`: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]`: Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `mac`: Perform MAC authentication if 802.1X authentication fails.

**Defaults**

By default, device classification is performed after the initial 802.1X authentication process fails.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Configuring the 802.1X authentication failure policy is not allowed on UNP ports on which 802.1X authentication bypass is enabled.

- Device classification (the default) is performed based on the classification options configured for the UNP port.

**Examples**

```
-> unp port 1/1/5 802.1x-authentication failure-policy mac
-> no unp port 1/1/10-15 802.1x-authentication failure-policy
```

```
-> unp linkagg 10 802.1x-authentication failure-policy mac
-> no unp linkagg 2-5 802.1x-authentication failure-policy
```
**Release History**
Release 7.3.4; command was introduced.

**Related Commands**

- `unp port-type`  
  Configures UNP functionality on a port or link aggregate.
- `unp 802.1x-authentication`  
  Configures the 802.1X authentication status for the UNP port.
- `unp 802.1x-authentication bypass-8021x`  
  Configures the 802.1X bypass operation status for the UNP port.
- `show unp port`  
  Displays the UNP configuration for the port.

**MIB Objects**

alaDaUNPPortTable
- alaDaUNPPort8021XFailurePolicy
**unp mac-authentication**

Configures the status of MAC authentication for the specified UNP port. Enable this functionality to invoke MAC-based authentication for devices connected to the UNP port.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} mac-authentication
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} mac-authentication
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

By default, MAC authentication is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable MAC authentication on a UNP port or link aggregate.
- This command is only allowed on UNP-enabled ports (both bridge and access port types).
- MAC-based authentication is supported only through a RADIUS server.
- An option exists to classify a device into an alternate UNP in the event successful MAC authentication does not return a UNP name.
- If MAC authentication fails, any classification rules configured for the UNP port are applied.
- If UNP MAC authentication, 802.1X authentication, and classification (see `unp classification` and `unp 802.1x-authentication`) are disabled on the UNP port, all MAC addresses received on that port are blocked unless a default UNP is configured and/or trust VLAN tag is enabled for the port.
- Configuring an authentication server down UNP (see `unp auth-server-down`) is highly recommended when MAC or 802.1X authentication is enabled on VLAN bridge or SPB access ports or aggregates. This is because after a switch reload, traffic from devices connected to these types of ports and
aggregates reaches the switch and triggers the authentication process before route convergence has
completed and the server can be reached.

– If an authentication server down UNP is configured, devices are temporarily learned in that profile
and authentication is automatically attempted again after the timeout period expires. This allows
time for the server to become reachable from the switch after a reload.

– If an authentication server down UNP is not configured, devices are learned as filtering and will
remain in that state. There is no further attempt to authenticate these devices again.

– The authentication server down functionality is not supported on VXLAN access ports or
aggregates.

Examples

-> unp port 1/1 mac-authentication
-> no unp port 1/1 mac-authentication
-> unp linkagg 2 mac-authentication
-> no unp linkagg 2 mac-authentication

Release History

Release 7.2.1; command was introduced.
Release 7.2.1.R02; linkagg parameter added.

Related Commands

unp port-type Configures UNP functionality on a port or link aggregate.
unp mac-authentication pass-
alternate Assigns the device to another VLAN-based or service-based UNP when successful MAC authentication does not return a UNP name.
unp classification Configures the classification status for the UNP port.
show unp port Displays the UNP configuration for the port.

MIB Objects

alaDaUNPPortTable
alaDaUNPPortIfIndex
alaDaUNPPortMacAuthFlag
**unp mac-authentication pass-alternate**

Configures the name of an existing VLAN-based or service-based UNP to use as an alternate profile. A device is assigned to the alternate profile when successful MAC authentication does not return a UNP name.

`unp {port chassis/slot/port1[{-port2}] | linkagg agg_id[-agg_id2]} mac-authentication pass-alternate profile_name`

`no unp {port chassis/slot/port1[{-port2}] | linkagg agg_id[-agg_id2]} mac-authentication pass-alternate`

### Syntax Definitions

- **chassis**
  The chassis identifier.

- **slot/port[{-port2}]**
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

- **profile_name**
  The name of an existing VLAN, SPB, or VXLAN profile.

### Defaults

By default, no alternate UNP is configured.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the alternate profile from the UNP port configuration.

- Service-based profiles classify traffic received on UNP access ports; VLAN-based profiles classify traffic received on UNP bridge ports. Make sure the specified port is of the correct type for the specified profile.

- The UNP name specified with this command must already exist in the switch configuration.

### Examples

```
-> unp port 1/1 mac-authentication pass-alternate Finance
-> unp port 1/1-3 mac-authentication pass-alternate CustomerA
-> unp port 1/4-10 mac-authentication pass-alternate CustomerC
-> no unp port 1/1-3 mac-authentication pass-alternate
```
-> unp linkagg 5 mac-authentication pass-alternate AltUNP
-> unp linkagg 1-5 mac-authentication pass-alternate CustomerB
-> unp linkagg 10-12 mac-authentication pass-alternate CustomerD
-> no linkagg 5 mac-authentication pass-alternate

**Release History**

Release 7.2.1; command was introduced.
Release 7.2.1.R02; `linkagg` parameter added.
Release 7.3.1; `spb-profile` parameter added, `unp-name` parameter changed to `vlan-profile`.
Release 7.3.4; `vxlan-profile` parameter added.
Release 8.3.1; `vlan-profile`, `spb-profile`, and `vxlan-profile` parameters deprecated.

**Related Commands**

- **unp profile**
  - Configures a UNP profile that is used to classify traffic received on UNP ports.

- **unp port-type**
  - Configures UNP functionality on a port or link aggregate.

- **unp mac-authentication**
  - Configures the MAC authentication status for the UNP port.

- **show unp port**
  - Displays the UNP port parameter configuration.

**MIB Objects**

- `alaDaUNPPortTable`
  - `alaDaUNPPortIfIndex`
  - `alaDaUNPPortPassAltProfileName`
**unp mac-authentication allow-eap**

Configures whether the switch attempts subsequent 802.1X authentication for a device connected to a UNP port on which 802.1X authentication bypass is enabled. When 802.1X bypass is enabled on the port, MAC authentication is performed first on any device connected to that port. This command specifies the conditions under which 802.1X authentication is performed or bypassed after the initial MAC authentication process.

```
unp {port chassis/slot/port1 [-port2] | linkagg agg_id[-agg_id2]} mac-authentication allow-eap {pass | fail | noauth}
```

```
no unp {port chassis/slot/port1 [-port2] | linkagg agg_id[-agg_id2]} mac-authentication allow-eap
```

**Syntax Definitions**

- **chassis**
  
  The chassis identifier.

- **slot/port [-port2]**
  
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id [-agg_id2]**
  
  Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

- **pass**
  
  Perform 802.1X (EAP frame) authentication if the device passes MAC authentication.

- **fail**
  
  Perform 802.1X (EAP frame) authentication if the device fails MAC authentication.

- **noauth**
  
  Perform 802.1X (EAP frame) authentication if MAC authentication is not configured on the UNP port.

**Defaults**

By default, the allow 802.1X authentication option is not set.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to set the allow 802.1X authentication option back to the default value of none (option is not set).

- The port specified with this command must also have 802.1X bypass enabled (see the `unp 802.1x-authentication bypass-8021x` command). If bypass is not enabled, the option configured with this command does not apply.
This command is only allowed on UNP-enabled ports and link aggregates.

**Examples**

-> unp port 1/1/5 mac-authentication allow-eap pass
-> unp port 1/1/10-15 mac-authentication allow-eap fail
-> no unp port 1/1/5 mac-authentication allow-eap
-> unp linkagg 10 mac-authentication allow-eap noauth
-> unp linkagg 2-5 mac-authentication allow-eap none
-> no unp linkagg 10 mac-authentication allow-eap

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- **unp port-type**
  - Configures UNP functionality on a port or link aggregate.

- **unp 802.1x-authentication bypass-8021x**
  - Configures the 802.1X bypass operation status for the UNP port.

- **show unp port**
  - Displays the UNP configuration for the port.

**MIB Objects**

- `alaDaUNPPortTable`
  - `alaDaUNPPortMacAllowEap`
**unp classification**

Configures the classification status for the specified UNP port. When classification is enabled but authentication is disabled or fails, UNP classification rules (such as MAC address, MAC address range, IP network address, or VLAN tag) are applied to the traffic received on the UNP port.

```
unp {port chassis/slot/port1 [-port2] | linkagg agg_id[-agg_id2]} classification

no unp {port chassis/slot/port1 [-port2] | linkagg agg_id[-agg_id2]} classification
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (10-20).

**Defaults**

By default, classification is enabled on the UNP port.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the classification status for a UNP port or link aggregate.
- This command is allowed only on UNP-enabled ports (both bridge and access ports).
- UNP classification rules are applied if authentication is disabled on the port, is enabled on the port but the RADIUS server is not configured, or the authentication method fails.
- If untagged device traffic does not match any of the classification rules, the device is assigned to the default UNP configured for the port.
- If tagged device traffic does not match any of the classification rules and the trust VLAN tag option (see `unp trust-tag`) is enabled for the port, the device is classified based on the VLAN tag of the traffic if a VLAN matching the tag exists in the switch configuration.
- If all of the UNP authentication methods and UNP classification are disabled for the UNP port, then all MAC addresses received on that port are blocked unless a default VLAN is specified and/or trust VLAN tag is enabled for the port.
• When classification is enabled for the port, UNP classification rules are applied in the following order of precedence:
  – MAC address + VLAN tag
  – MAC address
  – MAC address range + VLAN tag
  – MAC address range
  – IP address + VLAN tag
  – IP address
  – VLAN tag

Examples
-> unp port 1/1 classification
-> no unp port 1/1 classification
-> unp port 1/1-4 classification
ERROR: Port 1/3 is not a unp-port
-> unp linkagg 5 classification
-> no unp linkagg 5 classification

Release History
Release 7.2.1; command was introduced.
Release 7.2.1.R02; linkagg parameter added.

Related Commands
show unp classification Displays the UNP classification rule configuration for the switch.
show unp port Displays the UNP configuration for the port.

MIB Objects
alaDaUNPPortTable
  alaDaUNPPortIfIndex
  alaDaUNPPortClassificationFlag
**unp trust-tag**

Configures the option of whether or not to trust the VLAN ID of a tagged packet to determine how the packet is classified.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} trust-tag
```

```
no {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} trust-tag
```

**Syntax Definitions**

- `chassis` - The chassis identifier.
- `slot/port[-port2]` - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` - The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (10-20).

**Defaults**

By default, the trust VLAN tag option is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to disable the trust tag status for a UNP port or link aggregate.

- When this option is enabled, the device is classified into a VLAN or service access point (SAP) when one of the following conditions occur:
  - MAC or 802.1X authentication passes, but the RADIUS server returns a UNP that does not exist in the switch configuration.
  - MAC or 802.1X authentication passes, but the RADIUS server does not return a UNP and the alternate UNP option is disabled for the port.
  - Device traffic does not match any of the classification rules configured for the UNP port.
  - The UNP VLAN obtained from a matching classification rule does not exist in the switch configuration.
  - Auth-Server-Down UNP option is used, but the VLAN associated with that UNP does not exist in the switch configuration.

- When the trust tag option is triggered on a UNP bridge port and a VLAN exists in the switch configuration that matches the VLAN tag, a VLAN-port-association (VPA) is created between the UNP port and the matching VLAN even if the matching VLAN is _not_ associated with a UNP.
• When the trust tag option is triggered on a UNP access port, the VLAN tag information is used to create a dynamic SAP (virtual port) to which the access port is associated.

• Enabling the trust VLAN ID tag option provides an implicit method of VLAN tag classification that will accept tagged traffic matching any of the existing UNPs without the need to create specific classification rules for those profiles.

Examples

-> unp port 1/1 trust-tag
-> unp port 1/1-4 trust-tag
-> no unp port 1/1 trust-tag

-> unp linkagg 5 trust-tag
-> unp linkagg 6-10 trust-tag
-> no unp linkagg 5 trust-tag

Release History

Release 7.2.1; command was introduced.

Related Commands

show unp port         Displays the UNP configuration for the port.
show unp user         Displays information about the devices learned on a UNP port.

MIB Objects

alaDaUNPPortTable
    alaDaUNPPortIfIndex
    alaDaUNPPortTrustTagStatus
**unp default-profile**

Configures the name of an existing UNP classification profile to serve as the default UNP for the specified UNP port or link aggregate.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} default-profile profile_name
no unp {port chassis/slot/port1[-port2] | linkagg agg_id} default-profile
```

**Syntax Definitions**

- `chassis` The chassis identifier when running in virtual chassis mode.
- `slot/port[-port2]` The slot and port number (3/1) of a UNP-enabled port. Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `profile_name` The name of an existing UNP classification profile.

**Defaults**

By default, there is no default profile configured for UNP ports or link aggregates.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove the default UNP from the port configuration.
- This command is allowed only on UNP-enabled ports.
- The UNP classification profile specified with this command must already exist in the switch configuration.
- The default UNP is used to classify devices on the port when one of the following conditions occur:
  - UNP authentication and classification are not enabled on the port.
  - MAC authentication fails.
  - Device traffic does not match any UNP classification rules.
  - The UNP trust VLAN tag option (see `unp trust-tag`) is enabled for the port, but the VLAN ID specified in the tag field of the device traffic does not exist in the switch configuration.
  - Untagged device traffic is not classified.
**Examples**

-> unp port 1/1 default-profile Sales  
-> no unp port 1/1 default-profile  
-> unp port 1/1-4 default-profile Sales  
ERROR: Port 1/2 is not a unp port  
ERROR: Port 1/3 is not a unp port  
-> unp port 1/1 default-profile BAD-UNP  
ERROR: UNP doesn't exist  
-> no unp port 1/1-4 default-profile  
-> unp linkagg 5 default-profile VM1-Server1  
-> no unp linkagg 5 default-profile

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp profile**  
  Configures a UNP profile that is used to classify traffic received on UNP ports.

- **unp port-type**  
  Configures the status of UNP functionality on the port.

- **unp trust-tag**  
  Configures whether or not a device is classified into an existing VLAN that matches the VLAN ID tag of the packets received from the device.

- **show unp port**  
  Displays the UNP configuration for the port.

**MIB Objects**

alaDaUNPPortTable
  - alaDaUNPPortIfIndex
  - alaDaUNPPortDefaultProfileName
**unp domain**

Assigns a UNP port or link aggregate to a customer domain (UNP group).

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} domain domain_id
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} domain domain_id
```

### Syntax Definitions

**chassis**

The chassis identifier.

**slot/port[-port2]**

The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

**agg_id[-agg_id2]**

The link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

**domain_id**

The numerical domain ID to which the specified port or link aggregate is assigned.

### Defaults

By default, all UNP ports are assigned to customer domain zero (0).

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The domain ID specified with this command must already exist in the switch configuration.
- Customer domains are used to group physical UNP ports or link aggregates into one logical domain.
- Once a port is assigned to a specific customer domain, only classification rules associated with the same customer domain ID are applied to that port.

### Examples

- `-> unp port 1/1 domain 1`
- `-> unp port 1/1-3 domain 2`
- `-> no unp port 1/1 domain 1`
- `-> unp linkagg 5 domain 5`
- `-> unp linkagg 8-10 domain 6`
- `-> no unp linkagg 5 domain 5`
**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- `unp port-type`  
  Configures the status of UNP for the specified port or link aggregate.

- `unp domain description`  
  Creates a customer domain ID.

- `show unp domain`  
  Displays the available customer domain IDs.

- `show unp port`  
  Displays the UNP configuration for the port.

**MIB Objects**

- `alaDaUNPPortTable`  
  - `alaDaUNPPortIfIndex`
  - `alaDaUNPPortDomainId`
**unp aaa-profile**

Assigns the name of an existing authentication, authorization, and accounting (AAA) profile to the specified UNP port or link aggregate. This type of profile defines AAA configuration options (such as RADIUS servers and RADIUS client attributes) that are applied to device traffic received on the UNP port to which the profile is assigned.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} aaa-profile profile_name
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} aaa-profile
```

**Syntax Definitions**

- `chassis/slot/port1[-port2]`  
  The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).

- `agg_id[-agg_id2]`  
  The link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

- `profile_name`  
  The name of an existing AAA profile.

**Defaults**

By default, there is no AAA profile assigned to UNP ports or link aggregates. The global AAA configuration for the switch is applied.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8</th>
<th>6900C32E/T24C2</th>
<th>X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove the AAA profile from the port configuration.
- The AAA profile specified with this command must already exist in the switch configuration.
- AAA profiles are configured using the `aaa profile` command. See the “AAA Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide* for more information.

**Examples**

```
-> unp port 1/1/5 aaa-profile A1
-> no unp port 1/1/5 aaa-profile

-> unp port 1/1/1-5 aaa-profile A2
-> no unp port 1/1/1-5 aaa-profile

-> unp linkagg 10 aaa-profile A3
```
-> no unp linkagg 10 aaa-profile

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- **unp port-type**  
  Configures UNP functionality for the specified port or link aggregate.

- **aaa profile**  
  Configures an AAA configuration profile.

- **show unp port**  
  Displays the UNP configuration for the port.

**MIB Objects**

- **alaDaUNPPortTable**
  - **alaDaUNPPortIfIndex**
  - **alaDaUNPPortAaaProfile**
**unp port port-template**

Assigns the name of an existing port template to the specified UNP port or link aggregate. A port template defines UNP port configuration options (such as the type of authentication, classification status, a default profile) that are applied to the UNP port to which the template is assigned.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} port-template template_name
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} port-template
```

**Syntax Definitions**

- `chassis/slot/port1[-port2]` The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `template_name` The name of an existing port template.

**Defaults**

By default, the “bridgeDefaultPortTemplate” port template is assigned to UNP bridge ports, and the “accessDefaultPortTemplate” port template is assigned to UNP access ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of the command to remove the port template from the port configuration.
- When a custom template is removed from a UNP port, the port reverts back to using the default template to define UNP port parameter options.
- The port template specified with this command must already exist in the switch configuration.
- When a port template is applied to a UNP port, the parameter values defined in the template will override any existing UNP port configuration. In addition, any attempt to explicitly configure a port that is associated with a template is not allowed.

**Examples**

```
-> unp port 1/1/5 port-template up1
-> unp port 1/1/1-5 port-template up2
-> no unp port 1/1/5 port-template
-> no unp port 1/1/1-5 port-template
```
-> unp linkagg 10 port-template up3
-> unp linkagg 10-50 port-template up4
-> no unp linkagg 10 port-template
-> no unp linkagg 10-50 port-template
-> unp port 1/10 802.1x-authentication
ERROR: Port Template already enforced on port, please remove it for manual config on Port

Release History
Release 8.3.1; command was introduced.

Related Commands

unp port-type
Configures the UNP status and port type for the specified port or link aggregate.

unp port-template
Configures a port template.

show unp port config
Displays the UNP configuration for the port.

MIB Objects
alaDaUNPPortTable
alaDaUNPPortIfIndex
alaDaUNPPortPortTemplate
**unp direction**

Configures whether network access control is applied to both incoming and outgoing traffic or only applied to incoming traffic on the specified UNP bridge port or link aggregate.

```plaintext
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} direction {both | in}
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} direction
```

**Syntax Definitions**

- **chassis** The chassis identifier.
- **slot/port[-port2]** The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]** Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

- **both** Enables bidirectional network access control on the specified port or link aggregate.
- **in** Enables network access control for incoming traffic only on the specified port or link aggregate.

**Defaults**

By default, bidirectional network access control is enabled on the port.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C8/C32E/T24C2</th>
<th>6900X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to set the network access control direction to the default (**both**).
- When the port control direction is set to **both**, egress broadcast, unknown unicast, and multicast traffic is blocked on the UNP port.
- When the port control direction is set to **in**, egress broadcast, unknown unicast, and multicast traffic is allowed on the UNP port.
- This command applies only to ports and link aggregates configured as UNP bridge ports; this command does not apply to UNP access ports.

**Examples**

```plaintext
-> unp port 1/1/5 direction in
```
-> unp port 1/1/10-15 direction both
-> no unp port 1/1/10-15 direction
-> unp linkagg 10 direction in
-> unp linkagg 2-5 direction both
-> no unp linkagg 2-5 direction

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `unp port-type` Configures UNP functionality on a port or link aggregate.
- `unp 802.1x-authentication` Configures the 802.1X authentication status for the UNP port.
- `show unp port` Displays the UNP configuration for the port.

**MIB Objects**

- `alaDaUNPPortTable`
  - `alaDaUNPPortAdminControlledDirections`
unp admin-state

Enables or disables the UNP configuration for a port or link aggregate.

```
unp {port {chassis/slot/port1[-port2] | linkagg agg_id1[-agg_id2]} admin-state {enable | disable}
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id1[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (5-10).
- **enable**: Activates the UNP configuration for the UNP port or link aggregate. UNP functionality is applied to traffic received on the UNP port or link aggregate.
- **disable**: Disables the UNP configuration for the UNP port or link aggregate. UNP functionality is not applied to traffic received on the UNP port or link aggregate.

**Defaults**

By default, UNP is administratively enabled at the time UNP functionality is configured for the port or link aggregate.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When UNP functionality is disabled, the UNP configuration for the port or link aggregate is retained but is not applied to traffic received on the port or link aggregate.

**Examples**

- `unp port 1/1 admin-state disable`
- `unp port 1/2-5 admin-state disable`
- `unp port 1/1 admin-state enable`
- `unp linkagg 5 admin-state disable`
- `unp linkagg 8-10 admin-state disable`
- `unp linkagg t admin-state enable`
Release History
Release 8.3.1; command was introduced.

Related Commands

unp port-type
Configures UNP functionality for the specified port or link aggregate.

show unp port
Displays the UNP configuration for the port.

MIB Objects
alaDaUNPPortTable
alaDaUNPPortIfIndex
alaDaUNPPortAdminState
**unp dynamic-service**

Configures whether the System Default service profile dynamically creates an SPB Service Access Point (SAP) or a VXLAN SAP based on the traffic received on the UNP access port.

```
unp {port [chassis_id/|slot/port1]-port2] | linkagg agg_id[-agg_id2]} dynamic-service {spb | vxlan | none}
```

**Syntax Definitions**

- `chassis_id` The chassis identifier when running in virtual chassis mode.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `spb` Dynamically creates an SPB SAP.
- `vxlan` Dynamically creates a VXLAN SAP *(supported only on OmniSwitch 6900-X72/Q32 and OmniSwitch 6900-V72/C32)*.
- `none` No SPB or VXLAN SAP is dynamically created.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command applies only to ports and link aggregates configured as UNP access ports; this command does not apply to UNP bridge ports.

- Traffic received on UNP access ports that is not assigned to a user-defined service profile is assigned to the System Default service profile. The System Default profile attributes used to dynamically create a SAP for such traffic are derived based on the setting for this UNP port parameter.
  - If the dynamic service port parameter is set to SPB, then a calculated SPB control BVLAN, a calculated default I-SID number, and an incremental reserved service ID number are used to dynamically create a SAP for SPB service traffic received on the UNP access port.
  - If the dynamic service port parameter is set to VXLAN, then a calculated VNI number, a default multicast group IP address, and an incremental reserved service ID number are used to dynamically create a SAP for VXLAN service traffic received on the UNP access port.
**Examples**

-> unp port 1/1/5 dynamic-service vxlan
-> unp port 1/1/10-15 dynamic-service spb
-> unp port 1/1/10-15 dynamic-service none
-> unp linkagg 10 dynamic-service vxlan
-> unp linkagg 2-5 dynamic-service spb
-> unp linkagg 2-5 dynamic-service none

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- `unp port-type`  
  Configures UNP functionality on a port or link aggregate.
- `show unp port`  
  Displays the UNP configuration for the port.

**MIB Objects**

- `alaDaUNPPortTable`
  - `alaDaUNPPortDynamicService`
**unp vlan**

Configures an untagged or tagged VLAN-port association between the specified UNP bridge port and VLAN ID. This type of static VLAN assignment is particularly useful when connecting silent devices to UNP bridge ports.

```plaintext
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} vlan vlan_id [-vlan_id2] [tagged]
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} vlan vlan_id [-vlan_id2]
```

**Syntax Definitions**

- `chassis/slot/port1[-port2]`:
  The chassis ID, slot, and port number (3/1/1) for a specific UNP bridge port. Use a hyphen to specify a range of ports (3/1/1-8).

- `agg_id[-agg_id2]`:
  Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).

- `vlan_id [-vlan_id2]`:
  The VLAN ID to assign to the UNP port. Use a hyphen to specify a range of VLAN IDs.

- `tagged`:
  Configures a tagged VLAN association for the UNP bridge port.

**Defaults**

By default, no VLAN associations are configured for UNP bridge ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a VLAN association from the UNP port configuration. The `tagged` keyword is not required to remove a tagged VLAN association.

- This command applies only to ports and link aggregates configured as UNP bridge ports; this command does not apply to UNP access ports.

- When the `tagged` parameter option is not specified, the VLAN-port association created is untagged.

- Configuring a UNP port or link aggregate with an untagged and tagged VLAN-port association is allowed as long as the untagged and tagged VLANs are different (for example, `unp port 1/4/45 vlan 100` and `unp port 1/4/45 vlan 200 tagged`).

- When this command is used to assign a VLAN to a UNP bridge port, the port goes into a forwarding state for egress traffic associated with the VLANs assigned to the port. This automatically occurs even
when there is no MAC address learned on the UNP port in the assigned VLANs and regardless of the direction value (in or both) set for the port.

**Examples**

```
-> unp port 1/1/5 vlan 500
-> unp port 1/1/5 vlan 600 tagged
-> unp port 1/1/10 vlan 100-105
-> unp port 1/1/10 vlan 200-205 tagged
-> no unp port 1/1/5 vlan 500
-> no unp port 1/1/5 vlan 600
-> no unp port 1/1/10 vlan 100-105
-> no unp port 1/1/10 vlan 200-205

-> unp linkagg 10 vlan 500
-> unp linkagg 10 vlan 600 tagged
-> unp linkagg 20 vlan 100-105
-> unp linkagg 20 vlan 200-205 tagged
-> no unp linkagg 10 vlan 500
-> no unp linkagg 10 vlan 600
-> no unp linkagg 20 vlan 100-105
-> no unp linkagg 20 vlan 200-205
```

**Release History**

Release 8.2.1; command was introduced.
Release 8.5R4; **tagged** parameter added.

**Related Commands**

- **unp port-type**
  - Configures UNP functionality on a port or link aggregate.
- **show unp port configured-vlans**
  - Displays the VLAN assignments configured for UNP bridge ports or link aggregates.

**MIB Objects**

- alaDaUNPPortVlanTable
- alaDaUNPPortVlanVID
unp port profile

Configures a UNP service profile as a static profile for the specified UNP port. This type of profile assignment is particularly useful for silent devices that are connected to a UNP port; the profile SAP won’t age out when the device goes idle.

```
unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} profile profile_name
```

```
no unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} profile profile_name
```

**Syntax Definitions**

- **chassis/slot/port[-port2]** The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
- **agg_id[-agg_id2]** Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15).
- **profile_name** The name of an SPB, VXLAN, or L2 GRE service profile to statically assign to the specified UNP port.

**Defaults**

By default, no static profile is configured for UNP ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a static profile association from the UNP port configuration.

- When a MAC address is learned on a UNP port and classified into a service profile, a SAP is dynamically created based on the parameter values of the service profile. Once the MAC address associated with the dynamic SAP ages out, the SAP ages out as well. To accommodate silent devices, use this command to assign a service profile to the UNP port. This will dynamically create a persistent SAP that will not age out when the device MAC address ages out; the SAP continues to receive broadcast and multicast packets for the silent device.

- Make sure the specified UNP profile name already exists in the switch configuration and is mapped to an SPB, VXLAN, L2 GRE, or static service.
  - Profiles mapped to SPB, VXLAN, or static services are configured as static profiles on UNP access ports.
  - Profiles mapped to an L2 GRE service are configured as static profiles on UNP bridge or access ports.
• There can be up to eight SPB or VXLAN service profiles statically assigned to one UNP access port, but mixing service types on the same port is not supported. For example, configure only eight SPB service profiles or eight VXLAN service profiles.

• There can only be one L2 GRE service profile statically assigned to a UNP bridge or access port.

Examples

- unp port 1/1/5 profile static-spb1
- unp port 1/1/5 profile static-spb2
- unp port 1/1/10 profile static-vxlan1
- unp port 1/1/10 profile static-vxlan2
- unp port 1/20 profile static-l2gre1
- no unp port 1/20 profile static-l2gre1

- unp linkagg 10 profile static-spb1
- unp linkagg 20 profile static-vxlan1
- unp linkagg 30 profile static-l2gre1
- no unp linkagg 30 profile static-l2gre1

Release History

Release 8.5R4; command was introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp profile map service-type spb</td>
<td>Configures the mapping of SPB parameters to the specified UNP profile.</td>
</tr>
<tr>
<td>unp profile map service-type vxlan</td>
<td>Configures the mapping of VXLAN parameters to the specified UNP profile.</td>
</tr>
<tr>
<td>unp profile map service-type l2gre</td>
<td>Configures the mapping of an L2 GRE tunnel to the specified UNP profile.</td>
</tr>
<tr>
<td>unp profile map service-type static</td>
<td>Configures the mapping of an existing SPB or VXLAN service ID to the specified UNP profile.</td>
</tr>
<tr>
<td>show unp port profile</td>
<td>Displays the UNP service profiles that are statically assigned to UNP ports or link aggregates.</td>
</tr>
</tbody>
</table>

MIB Objects

alaDaUNPPortTable
alaDaUNPPortProfile
**unp port ap-mode**

Configures the status of the Access Point (AP) mode for the specified UNP port or link aggregate.

```
unp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} ap-mode {secure}
no unp {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} ap-mode {secure}
```

### Syntax Definitions

- **chassis/slot/port[-port2]**: The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number for a specific UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).
- **secure**: Set the secure ap-mode configuration on port enabled or disabled.

### Defaults

By default, the AP mode status for the port or link aggregate is set to the global AP mode status when UNP is enabled on the port or link aggregate. For example, if the global status is disabled, the port-level status is initially disabled. Secure ap-mode is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- AP mode functionality is supported on UNP bridge ports and on UNP access ports. On bridge ports, the AP device and AP clients are learned into the VLAN domain; on access ports, the AP device and AP clients are learned into the Shortest Path Bridging (SPB) service domain.

- When the AP mode is enabled on the specified UNP bridge port and an AP device is detected on that port, the following actions are triggered to automatically change the operational status of the specified options (the operational status overrides the configured status):
  - The transmission of LLDP Port VLAN ID and AP Location TLVs is operationally enabled on the UNP bridge port.
  - The trust tag status for the UNP bridge port is operationally enabled.
  - The global status for dynamic VLAN configuration is operationally enabled for the switch.

- When the AP mode is enabled on a UNP access port and an AP device is detected on that port, the following actions are triggered to automatically change the operational status of the specified options (the operational status overrides the configured status):
The transmission of LLDP Port VLAN ID and AP Location TLVs is operationally enabled on the UNP access port.

The trust tag function is not used; AP clients are not learned into VLAN-based profiles. Instead, AP clients are learned into a UNP profile that is mapped to SPB service parameters. The SAP that is dynamically created based on the service parameters carries the AP client traffic.

MAC or 802.1X authentication is bypassed for AP clients. However, the other Layer 2 UNP port options for learning and assigning an AP client to a profile are available, such as rule classification, a default SPB service profile, or a dynamic SPB System Default profile.

- Once the AP MAC address is detected and learned, a built-in LLDP UNP classification rule for access points classifies the AP device into one of the following built-in default profiles:
  - **defaultWLANProfile** for AP devices connected to UNP bridge ports. This profile is mapped to a VLAN into which the AP device is classified. A VLAN-port association (VPA) is established between the UNP bridge port and profile VLAN on which the AP MAC address is learned and forwarded.
  - **defaultWLANAccessProfile** for AP devices connected to UNP access ports. The profile is mapped to SPB service parameters. When the AP device is classified into this profile, an SPB Service Access Point (SAP) is dynamically created. A SAP-port association is established between the UNP access port and the SAP on which the AP MAC address is learned and forwarded.

- If the UNP AP mode is not enabled, the detection, learning, and management of connected OmniAccess Stellar AP devices may not occur as expected.

- AP mode functionality is not supported on Learned Port Security (LPS) ports.

- Use **secure** parameter to enable or disable the secure ap-mode.

**Examples**

- `unp port 1/1/6 ap-mode`
- `unp linkagg 10 ap-mode`
- `no unp port 1/1/6 ap-mode`
- `no unp linkagg 10 ap-mode`
- `unp port 1/1/1 ap-mode secure`
- `no unp port 1/1/1 ap-mode secure`

**Release History**

Release 8.6R1; command was introduced.
Release 8.81R1; **secure** parameter added

**Related Commands**

- **unp ap-mode** Configures the global AP mode status.
- **show unp port config** Displays the UNP configuration for the port.
- **show unp global configuration** Displays the status of UNP Layer 3 learning for the switch.

**MIB Objects**

- alaDaUNPPortTable
- alaDaUNPPortApMode
- alaDaUNPPortApModeSecurity
unp port-template

Configures a UNP port template that is used to apply a pre-defined port configuration to a UNP port or link aggregate. Using a port template to configure UNP functionality on a port or link aggregate avoids having to configure each parameter with a separate CLI command. Applying a template configures all port-based parameters with a single CLI command.

This section describes the base command (unp port-template) along with optional command keywords that are used to configure port parameter values that are applied when the template is assigned to a UNP port or link aggregate. Optional keywords are listed separately but can be entered in combination on the same command line. Use the no form for the keywords to change a specific parameter value for the template.

There are two default port templates: “bridgeDefaultPortTemplate” (applied to UNP bridge ports) and “accessDefaultPortTemplate” (applied to UNP access ports). These templates define a default set of port parameter values that are applied at the time a port or link aggregate is configured as a UNP bridge or access port. The default templates cannot be deleted, but the template parameter values are configurable through this command.

unp port-template {template_name | bridgeDefaultPortTemplate | accessDefaultPortTemplate}
   [802.1x-authentication]
   [802.1x-authentication pass-alternate profile_name]
   [mac-authentication]
   [mac-authentication pass-alternate profile_name]
   [classification]
   [trust-tag]
   [default-profile profile_name]
   [domain domain_id]
   [aaa-profile profile_name]
   [redirect port-bounce]
   [direction {in | both}]
   [802.1x-authentication tx-period seconds]
   [802.1x-authentication supp-timeout seconds]
   [802.1x-authentication max-req max_req]
   [802.1x-authentication bypass]
   [802.1x-authentication failure-policy {mac}]
   [mac-authentication allow-eap {pass | fail | noauth}]
   [force-l3-learning {port-bounce}]
   [admin-state {enable | disable}]
   [dynamic-service {spb | vxlan}]
   [vlan vlan_id [-vlan_id2] [tagged]]
   [l2-profile l2profile_name]
   [profile profile_name]
   [ap-mode][secure]

no unp port-template template_name [802.1x-authentication | 802.1x authentication pass-alternate | mac-authentication | mac-authentication pass-alternate | ...]
**Syntax Definitions**

- `template_name` - The name to associate with the UNP port template.
- `bridgeDefaultPortTemplate` - The name of the default port template applied to UNP bridge ports.
- `accessDefaultPortTemplate` - The name of the default port template applied to UNP access ports. *This parameter is currently not supported on an OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*

**Defaults**

The following table contains the default values for the system-defined port templates (“accessDefaultPortTemplate” and “bridgeDefaultPortTemplate”):

<table>
<thead>
<tr>
<th>parameter</th>
<th>system-defined port template values</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x-authentication</td>
<td>enabled</td>
</tr>
<tr>
<td>802.1x-authentication pass-alternate profile_name</td>
<td>none</td>
</tr>
<tr>
<td>mac-authentication</td>
<td>enabled</td>
</tr>
<tr>
<td>mac-authentication pass-alternate profile_name</td>
<td>none</td>
</tr>
<tr>
<td>classification</td>
<td>enabled</td>
</tr>
<tr>
<td>trust-tag</td>
<td>disabled</td>
</tr>
<tr>
<td>default-profile profile_name</td>
<td>none</td>
</tr>
<tr>
<td>domain domain_id</td>
<td>0</td>
</tr>
<tr>
<td>aaa-profile profile_name</td>
<td>none</td>
</tr>
<tr>
<td>redirect port-bounce</td>
<td>disabled</td>
</tr>
<tr>
<td>direction {in</td>
<td>both}</td>
</tr>
<tr>
<td>802.1x-authentication tx-period seconds</td>
<td>30</td>
</tr>
<tr>
<td>802.1x-authentication supp-timeout seconds</td>
<td>30</td>
</tr>
<tr>
<td>802.1x-authentication max-req max_req</td>
<td>2</td>
</tr>
<tr>
<td>802.1x-authentication bypass</td>
<td>disabled</td>
</tr>
<tr>
<td>802.1x-authentication failure-policy {mac}</td>
<td>default</td>
</tr>
<tr>
<td>mac-authentication allow-eap {pass</td>
<td>fail</td>
</tr>
<tr>
<td>force-l3-learning [port-bounce]</td>
<td>disabled port bounce is enabled</td>
</tr>
<tr>
<td>admin state {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>dynamic-service {vxlan</td>
<td>spb}</td>
</tr>
<tr>
<td>vlan vlan_id [-vlan_id2] [tagged]</td>
<td>none</td>
</tr>
<tr>
<td>l2-profile l2profile_name</td>
<td>unp-def-access-profile</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove a port template from the switch configuration.

- To change the value of a specific port template parameter, specify the parameter keyword with this command. For example, no unp port-template port1 mac-authentication, unp port-template port1 domain 2, or unp port-template port1 default-profile defprof1. The new parameter values are applied to all UNP ports to which the template is assigned.

- The l2-profile port template parameter is not supported on the OmniSwitch 9900.

- If the name of the template does not exist when this command is used to modify a port parameter, the switch will automatically create a new template using the name specified. For example, the unp port-template port1 mac-authentication command will create the “port1” template if it does not already exist in the switch configuration.

- When a port template is applied to a UNP port, the parameter values defined in the template will override any existing UNP port configuration. In addition, any attempt to explicitly configure a port that is associated with a template is not allowed.

- For more information about specific port parameter values, refer to the following explicit UNP port configuration commands for each template parameter:

<table>
<thead>
<tr>
<th>Port Template Parameter</th>
<th>Explicit Port Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>[802.1x-authentication]</td>
<td>unp 802.1x-authentication</td>
</tr>
<tr>
<td>[802.1x-authentication pass-alternate profile_name]</td>
<td>unp 802.1x-authentication pass-alternate profile_name</td>
</tr>
<tr>
<td>[mac-authentication]</td>
<td>unp mac-authentication</td>
</tr>
<tr>
<td>[mac-authentication pass-alternate profile_name]</td>
<td>unp mac-authentication pass-alternate profile_name</td>
</tr>
<tr>
<td>[classification]</td>
<td>unp classification</td>
</tr>
<tr>
<td>[default-profile profile_name]</td>
<td>unp default-profile</td>
</tr>
<tr>
<td>[domain domain_id]</td>
<td>unp domain</td>
</tr>
<tr>
<td>[aaa-profile profile_name]</td>
<td>unp aaa-profile</td>
</tr>
</tbody>
</table>
## Port Template Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>[redirect port-bounce]</td>
<td>unp redirect port-bounce</td>
</tr>
<tr>
<td>[direction {in</td>
<td>both}]</td>
</tr>
<tr>
<td>[802.1x-authentication tx-period seconds]</td>
<td>unp 802.1x-authentication tx-period</td>
</tr>
<tr>
<td>[802.1x-authentication supp-timeout seconds]</td>
<td>unp 802.1x-authentication supp-timeout</td>
</tr>
<tr>
<td>[802.1x-authentication max-req max_req]</td>
<td>unp 802.1x-authentication max-req</td>
</tr>
<tr>
<td>[802.1x-authentication bypass]</td>
<td>unp 802.1x-authentication bypass-8021x</td>
</tr>
<tr>
<td>[802.1x-authentication failure-policy {mac}]</td>
<td>unp 802.1x-authentication failure-policy</td>
</tr>
<tr>
<td>[mac-authentication allow-eap {pass</td>
<td>fail</td>
</tr>
<tr>
<td>[force-l3-learning {port-bounce}]</td>
<td>unp force-l3-learning</td>
</tr>
<tr>
<td>[trust-tag]</td>
<td>unp trust-tag</td>
</tr>
<tr>
<td>[admin-state {enable</td>
<td>disable}]</td>
</tr>
<tr>
<td>[dynamic-service {spb</td>
<td>vxlan}]</td>
</tr>
<tr>
<td>[vlan vlan_id [-vlan_id2] [tagged]]</td>
<td>unp vlan</td>
</tr>
<tr>
<td>[l2-profile l2profile_name]</td>
<td>unp l2-profile</td>
</tr>
<tr>
<td>[ap-mode]</td>
<td>unp port ap-mode</td>
</tr>
<tr>
<td>[profile profile_name]</td>
<td>unp port profile</td>
</tr>
</tbody>
</table>

## Examples

- `-> unp port-template port1`
- `-> unp port-template port1 mac-authentication`
- `-> unp port-template port1 mac-authentication pass-alternate unp1`
- `-> unp port-template port1 classification`
- `-> no unp port-template port1 mac-authentication`
- `-> no unp port-template port1`
- `-> unp port-template port2 802.1x-authentication`
- `-> unp port-template port2 classification`
- `-> unp port-template port2 domain 10`
- `-> no unp port-template port2 classification`
- `-> no unp port-template port2`
- `-> unp port-template pt1 ap-mode secure`
- `-> no unp port-template pt1 ap-mode secure`

## Release History

Release 8.3.1; command was introduced.
Release 8.3.1.R02; `force-l3-learning` parameter added.
Release 8.4.1; `l2-profile` parameter added.
Release 8.5R4; `profile` parameter added, `tagged` option added to `vlan` parameter.
Release 8.6R1; `ap-mode` parameter added.
Release 8.8R1; `secure` parameter added.
Related Commands

unp port port-template
Assigns a port configuration template to a UNP port.

show unp port config
Displays the UNP configuration for the port, including the name of the port template associated with the port, if any.

show unp port-template
Displays the port template configuration.
**MIB Objects**

alaDaUNPPortTemplateTable
alaDaUNPPortTemplateName
alaDaUNPPortTemplateAdminState
alaDaUNPPortTemplateDirection
alaDaUNPPortTemplateDomainID
alaDaUNPPortTemplateClassification
alaDaUNPPortTemplateTrustTag
alaDaUNPPortTemplateDynamicService
alaDaUNPPortTemplateDefaultProfile
alaDaUNPPortTemplateAAAProfile
alaDaUNPPortTemplateRedirectPortBounce
alaDaUNPPortTemplate8021XAuth
alaDaUNPPortTemplate8021XAuthPassAlternate
alaDaUNPPortTemplate8021XAuthBypass
alaDaUNPPortTemplate8021XAuthFailPolicy
alaDaUNPPortTemplate8021XAuthTxPeriod
alaDaUNPPortTemplate8021XAuthSuppTimeout
alaDaUNPPortTemplate8021XAuthMaxReq
alaDaUNPPortTemplateMACAuth
alaDaUNPPortTemplateMACAuthPassAlternate
alaDaUNPPortTemplateMACAuthAllowEAP
alaDaUNPPortTemplateForceL3Learning
alaDaUNPPortTemplateForceL3LearningPortBounce
alaDaUNPPortTemplateL2Profile
alaDaUNPPortTemplateApMode
alaDaUNPPortTemplateApModeSecurity
alaDaUNPPortTemplateVlanTable
alaDaUNPPortTemplateVlanVID
alaDaUNPPortTemplateProfileTable
alaDaUNPPortTemplateProfile
**unp network-group**

Configures a network group name and its associated IPv4 addresses. The group is used to specify source or destination IP networks for UNP router domain authentication. Users attempting to access networks defined in this group are challenged for authentication.

```
unp network-group net_group_name ip_address [mask net_mask] [ip_address2 [mask net_mask2]...]
no unp network-group net_group_name [ip_address [mask net_mask] [ip_address2 [mask net_mask2]...]
```

### Syntax Definitions

- `net_group_name`: The name of the network group (up to 31 alphanumeric characters).
- `ip_address`: An IPv4 address included in the network group.
- `net_mask`: The mask for the IPv4 address. If no mask is entered, the IPv4 address is assumed to be a host address.
- `ip_address2`: Optional. Another IPv4 address to be included in the network group. Multiple IPv4 addresses (up to a maximum of five) may be configured for a network group. Separate each address/mask combination with a space.
- `net_mask2`: Optional mask for the IPv4 address. If no mask is entered, the natural mask for the address will be used.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of the command to remove a network group from the configuration or to remove an IP address from a network group.
- The network group defined with this command is used to configure a router authentication condition that will trigger authentication for user traffic that matches the IPv4 networks defined in the group.
- Make sure that the IP networks/masks specified for a network group do not overlap.

### Examples

```
-> unp network-group net-grpl 10.10.12.5 mask 255.255.0.0
```
-> unp network-group net-grp1 20.10.12.5 mask 255.255.0.0 10.50.3.1
-> unp network-group net-grp1 30.12.12.5
-> unp network-group net-grp1 10.10.12.5 mask 255.255.0.0 10.50.3.1 30.12.12.5
-> no unp network-group net-grp1 10.10.12.5
-> no unp network group net-grp1

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- **unp router-auth user-group**
  Configures a user group as a condition for Layer 3 authentication. A network group is specified when this type of condition is configured.

- **unp router-auth cp-profile**
  Configures a Captive Portal profile for router authentication.

- **unp router-auth user flush**
  Performs a MAC address flush of the specified router domain authentication users.

- **show unp network-group**
  Displays the UNP network group configuration.

**MIB Objects**

- `alaDaUNPNetworkGroupTable`
  - `alaDaUNPNetworkGroupName`
  - `alaDaUNPNetworkGroupIpAddrType`
  - `alaDaUNPNetworkGroupIpAddr`
  - `alaDaUNPNetworkGroupIpMask`
**unp router-auth user-group**

Configures a user group as a condition for Layer 3 authentication. A user group specifies a destination network group and an optional source network group; traffic matching the networks in these groups is subject to router domain authentication.

```
unp router-auth user-group user_group_name {[src-network-group net_group] dst-network-group net_group_name}
```

```
no unp router-auth user-group user_group_name
```

**Syntax Definitions**

- **user_group_name**: The name of the router authentication condition (up to 31 alphanumeric characters).
- **net_group_name**: The name of an existing network group (configured through the `unp network-group` command).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of the command to remove a router authentication user group from the switch configuration.
- Make sure the network group specified with this command exists in the switch configuration before attempting to configure the router authentication user group.
- To configure an optional source network group; specify the source network group name first then the destination network group name.
- When the first router authentication user group is configured, the router domain authentication feature is enabled for the switch.
- HTTP/HTTPS traffic that matches a user group condition is challenged with Captive Portal authentication; other IPv4 traffic that matches a user group condition is challenged with IP-based authentication.
• Configuring multiple router authentication user groups is allowed.
  – Any two user groups can share the same source network group as long as the destination network
group for each user group is different and the IP addresses do not overlap.
  – Any two user groups can share the same destination network group as long as the source network
group for each user group is different and the IP addresses do not overlap.

Examples

- unp router-auth user-group ra-ugrp1 src-network-group net-grp1 dst-network-group net-grp2
- unp router-auth user-group ra-ugrp2 dst-network-group net-grp3

- no unp router-auth user-group ra-ugrp1
- no unp router-auth user-group ra-ugrp2

- unp router-auth user-group ra-ugrp1 dst-network-group grp5
  ERROR: Dst Network Group does not exist
- unp router-auth user-group ra-ugrp2 src-network-group grp5 dst-network-group net-grp2
  ERROR: Src Network Group does not exist

Release History

Release 8.5R4; command was introduced.

Related Commands

unp network-group Configures a network group name and its associated IPv4 addresses.
unp router-auth cp-profile Configures a Captive Portal profile for router authentication.
unp router-auth user flush Performs a MAC address flush of the specified router domain
  authentication users.
show unp router-auth user-
  group Displays the router authentication user group configuration.

MIB Objects

alaDaUNPRouterAuthUserGroupTable
  alaDaUNPRouterAuthenticationName
  alaDaUNPRouterAuthenticationSrcGroup
  alaDaUNPRouterAuthenticationDestGroup
unp router-auth cp-profile

Specifies an existing Captive Portal (CP) profile to use for router authentication. This type of profile defines CP authentication parameter options that are applied to users that match router authentication user group conditions. If no CP profile is specified, then the global CP configuration is applied.

`unp router-auth cp-profile cp_profile_name`

`no unp router-auth cp-profile cp_profile_name`

Syntax Definitions

`cp_profile_name` The name of an existing CP profile (configured through the captive-portal-profile command).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of the command to remove the CP profile assignment.
- Make sure the CP profile name specified with this command exists in the switch configuration.
- The following global and CP profile settings are applied for CP authentication:
  - The RADIUS server to use for authentication.
  - Session timeout value (determines aging of an accept/deny entry).
  - CP maximum retry attempts (number of login attempts the user is given before access is blocked).
  - Success redirect URL (the URL to display to the client after successful CP authentication)
- The following global and CP profile settings are applied for IP-based authentication:
  - The RADIUS server to use for authentication.
  - Session timeout value (determines aging of an accept/deny entry).
- If the RADIUS server returns a session timeout value that is set to zero and the trust RADIUS option is enabled, then the session timeout for CP and IP authenticated users is set to infinity (the user session does not time out). A zero session timeout value is supported only when it is returned by the RADIUS server; setting the value to zero through the CLI is not supported.
• The router domain authentication feature is not enabled for the switch until at least one router authentication user group is configured.

• CP authentication is applied to HTTP/HTTPS traffic that matches a router authentication user group condition.

Examples

-> unp router-auth cp-profile cp-1
-> no unp router-auth cp-profile

Release History

Release 8.5R4; command was introduced.

Related Commands

unp network-group
Configures a network group name and its associated IPv4 addresses.

unp router-auth user-group
Configures a user group as a condition for Layer 3 authentication. A network group is specified when this type of condition is configured.

unp router-auth user flush
Performs a MAC address flush of the specified router domain authentication users.

show unp router-auth configuration
Displays the CP profile configuration that is used for router domain authentication.

MIB Objects

alaDaUNPRouterAuthenticationConfig
alaDaUNPRouterAuthCpProfileName
**unp router-auth user flush**

Performs a MAC address flush of the specified router domain authentication users.

`unp router-auth user flush user-group user_group_name | user-name cp_user_name | [ip-address ipv4_address] | auth-type {cp | ip} | all`

---

**Syntax Definitions**

- `user_group_name`: The name of an existing router authentication user group.
- `cp_user_name`: The Captive Portal (CP) user name.
- `ipv4_address`: The IPv4 address associated with the router authentication user.
- `cp`: Clears only the CP-authenticated users.
- `ip`: Clears only the IP-authenticated users.
- `all`: Clears all of the router authentication users.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `user-group` parameter to flush all users associated with the specified router authentication user group.
- Use the `user-name` parameter to flush the CP user name associated with the router authentication user.
- Use the `ip-address` parameter to flush the IPv4 address associated with the router authentication user.
- Use the `auth-type` parameter with the `cp` or `ip` options to flush router authentication users that were authenticated through Captive Portal or IP-based mechanisms.
- Use the `all` parameter to flush all router authentication users learned on the switch.

---

**Examples**

- `-> unp router-auth user flush all`
- `-> unp router-auth user flush user-group ra-grp1`
- `-> unp router-auth user flush user-name san`
- `-> unp router-auth user flush ip-address 10.0.0.1`
- `-> unp router-auth user flush auth-type cp`
-> unp router-auth user flush auth-type ip

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- **unp network-group**  
  Configures a network group name and its associated IPv4 addresses.
- **unp router-auth user-group**  
  Configures a user group as a condition for Layer 3 authentication. A network group is specified when this type of condition is configured.
- **unp router-auth cp-profile**  
  Configures a Captive Portal profile for router authentication.
- **show unp router-auth users**  
  Displays information about users authenticating through router domain authentication.

**MIB Objects**

alaDaUNPRouterAuthenticationFlushTable
  - alaDaUNPRouterAuthenticationFlushIndex
  - alaDaUNPRouterAuthenticationFlushComplete
  - alaDaUNPRouterAuthenticationFlushUserGroupName
  - alaDaUNPRouterAuthenticationFlushType
  - alaDaUNPRouterAuthenticationFlushUserName
  - alaDaUNPRouterAuthenticationFlushIpAddressType
  - alaDaUNPRouterAuthenticationFlushIpAddress
show unp network-group

Displays the router authentication network group configuration.

show unp network-group

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

A UNP network group is used to configure a router authentication user group condition that will trigger authentication for user traffic that matches the IPv4 networks defined in the network group.

Examples

```
-> show unp network-group
  Network Group Name     IP-Address/Mask
-----------------------+----------------------------------
  net-grp1              10.0.0.1/255.255.0.0, 20.0.0.1/255.255.0.0, 30.0.0.1/255.0.0.0
  net-grp2              40.0.0.1/255.255.0.0
  net-grp3              10.0.0.1/255.255.0.0, 40.0.0.1/255.255.0.0

Total Network-Group Count: 3
```

Output definitions

- **Network Group Name**: The name of the UNP network group.
- **IP-Address/Mask**: The IPv4 network addresses that are associated with the network group name.

Release History

Release 8.5R4; command was introduced.
Related Commands

unp network-group  Configures a network group name and its associated IPv4 addresses.

MIB Objects

alaDaUNPNetworkGroupTable
  alaDaUNPNetworkGroupName
  alaDaUNPNetworkGroupIpAddrType
  alaDaUNPNetworkGroupIpAddr
  alaDaUNPNetworkGroupIpMask
**show unp router-auth user-group**

Displays the router authentication user group configuration.

**show unp router-auth user-group** [user_group_name]

### Syntax Definitions

user_group_name

The name of an existing router authentication user group.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

A router authentication user group specifies Layer 3 conditions for authentication; UNP network groups assigned to the router authentication user group contain IPv4 addresses. User traffic matching these networks are challenged with Captive Portal or IP-based authentication.

### Examples

```plaintext
-> show unp router-auth user-group
User-Group Name       Src-Network-Group       Dst-Network-Group
------------------------------+-----------------+-------------------
ra-ugrp1                net-grp1            net-grp2
ra-ugrp2                net-grp3            net-grp2
ra-ugrp3                net-grp1            net-grp3
ra-ugrp4                net-grp2            net-grp3
ra-ugrp5                net-grp2            net-grp4

-> show unp router-auth user-group UserGrp1
User-Group Name       Src-Network-Group       Dst-Network-Group
------------------------------+-----------------+-------------------
ra-ugrp3                net-grp1            net-grp3

Rule Status = ACTIVE
```

### output definitions

User-Group-Name The name of the router authentication user group.
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src-Network-Group</td>
<td>The name of the UNP network group that is designated as a group of source IPv4 networks. Specifying a source network group is optional when configuring a user group condition.</td>
</tr>
<tr>
<td>Dst-Network-Group</td>
<td>The name of the UNP network group that is designated as a group of destination IPv4 networks.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- `unp router-auth user-group` Configures a router authentication user group.

**MIB Objects**

- `alaDaUNPRouterAuthUserGroupTable`  
  - `alaDaUNPRouterAuthenticationName`  
  - `alaDaUNPRouterAuthenticationSrcGroup`  
  - `alaDaUNPRouterAuthenticationDestGroup`
show unp router-auth configuration

Displays the Captive Portal (CP) profile configuration that is used for router domain authentication.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If no CP profile is designated for this feature, then the global CP configuration is used.

Examples

-> show unp router-auth configuration
   CP-Profile Name : cp-prof1

   CP Params:
   Captive Portal AAA Profile Name = a1
   Captive Portal Success Redirect URL = http://server-1.com/pass.html
   Captive Portal Retry Count = 3

output definitions

<table>
<thead>
<tr>
<th>CP-Profile Name</th>
<th>The name of the Captive Portal profile to use for router authentication. Configured through the captive-portal-profile command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Captive Portal AAA Profile Name</td>
<td>The name of the AAA profile assigned to the CP profile. The AAA profile defines the session timeout value. Configured through the captive-portal-profile command.</td>
</tr>
<tr>
<td>Captive Portal Success Redirect URL</td>
<td>The URL to which a user is redirected after successful CP authentication. Configured through the captive-portal-success-redirect-url command.</td>
</tr>
<tr>
<td>Captive Portal Retry Count</td>
<td>The number of login attempts a client is allowed. Configured through the captive-portal retry-count command.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

`unp router-auth cp-profile` Specifies an existing CP profile to use for router authentication.

**MIB Objects**

`alaDaUNPRouterAuthenticationConfig`  
`alaDaUNPRouterAuthCpProfileName`
show unp router-auth users

Displays information about users authenticating through the router authentication process.

show unp router-auth users [user-name cp_user_name] [ip-address ipv4_address] [auth-type {cp | ip}] [auth-status {pass | fail}]

Syntax Definitions

- cp_user_name: The Captive Portal (CP) user name for the router authentication user.
- ipv4_address: The IPv4 address of the router authentication user.
- cp: Displays only Captive Portal authenticated users.
- ip: Displays only IP authenticated users.
- pass: Displays only users that have successfully authenticated.
- fail: Displays only users that have failed authentication.

Defaults
By default, all router authenticated users are displayed.

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the optional parameters provided with this command to filter the output display results.
- The “Username” field displays either the user name that was entered to authenticate a user device through the Captive Portal process or the IP address of the user device if IP-authentication was used to authenticate the user.

Examples

```
-> show unp router-auth users

UserName           Destination   User-Group Intf-Name/      Auth  Auth   LoginTime
                   IP-Network                Vlan      Type   Status
---------+-----------------+-----------+---------+-------+-------------------+-------------------+-------+-------------------+-------------------+-------+-------------------+-------------------+-------+-------------------+-------------------+-------+-------------------+-------------------+-------+
Guest-user1       70.0.0.1      DST-GRP1    L3-auth1:20  CP   Pass  06/20/2018 06:43:47
Employee-002      70.0.0.2      DST-GRP2    L3-auth2/30  CP   Fail  06/50/2018 02:00:02
40.1.1.20          70.0.0.3      DST-GRP3    L3-auth3/40  IP   Fail  07/20/2018 10:10:05
50.1.1.20          70.0.0.4      DST-GRP4    L3-auth4/50  IP   Pass  07/10/2018 05:14:10

Total users : 4
```
Access Guardian Commands

`show unp router-auth users`

```
-> show unp router-auth users ip-address 40.1.1.20
   UserName   Destination    User-Group Intf-Name/ Vlan Type Status
   IP-Network                  Vlan      Type Status
  +---------------------------------+----------+-----------+----+-------+-------------------
40.1.1.20     70.0.0.3       DST-GRP3   L3-auth3/40  IP   Fail  07/20/2018 10:10:05
Total users : 1
```

```
-> show unp router-auth users auth-type cp
   UserName   Destination    User-Group Intf-Name/ Vlan Type Status
   IP-Network                  Vlan      Type Status
  +---------------------------------+----------+-----------+----+-------+-------------------
Guest-user1   70.0.0.1       DST-GRP1   L3-auth1:20  CP   Pass  06/20/2018 06:43:47
Employee-002  70.0.0.2       DST-GRP2   L3-auth2/30  CP   Fail  06/50/2018 02:00:02
Total users : 2
```

```
-> show unp router-auth users auth-status pass
   UserName   Destination    User-Group Intf-Name/ Vlan Type Status
   IP-Network                  Vlan      Type Status
  +---------------------------------+----------+-----------+----+-------+-------------------
Guest-user1   70.0.0.1       DST-GRP1   L3-auth1:20  CP   Pass  06/20/2018 06:43:47
50.1.1.20     70.0.0.4       DST-GRP4   L3-auth4/50  IP   Pass  07/10/2018 05:14:10
Total users : 2
```

**output definitions**

<table>
<thead>
<tr>
<th><strong>UserName</strong></th>
<th>Displays either the IP address or Captive Portal user name for the learned user device.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination IP-Network</strong></td>
<td>The destination IP network address for the user device.</td>
</tr>
<tr>
<td><strong>User-Group</strong></td>
<td>The name of the router authentication user group condition that matches the user device traffic.</td>
</tr>
<tr>
<td><strong>Intf-Name/VLAN</strong></td>
<td>The name of the IP interface and VLAN associated with the user device.</td>
</tr>
<tr>
<td><strong>Auth Type</strong></td>
<td>Indicates whether the user device attempted Captive Portal or IP-based authentication.</td>
</tr>
<tr>
<td><strong>Auth Status</strong></td>
<td>Indicates whether the user device passed or failed authentication.</td>
</tr>
<tr>
<td><strong>LoginTime</strong></td>
<td>The date and time the user logged into the network.</td>
</tr>
</tbody>
</table>

```
-> show unp router-auth users user-name Guest-user1
   User-Name : Guest-user1
   IP-Address : 20.0.0.5,
   Destination IP-Network : 70.0.0.1,
   Access Timestamp : 06/20/2018 06:43:47,
   Interface-Name/Vlan : L3-auth1/20,
   User-Group : DST-GRP1,
   Authentication-Type : CP,
   Authentication-Status : Pass,
   Session-Time Remaining(sec) : 1000 sec
```
-> show unp router-auth users user-name 40.1.1.20

User-Name : 40.1.1.20
IP-Address : 40.1.1.20,
  Destination IP-Network : 70.0.0.0,
  Access Timestamp : 07/20/2018 10:10:05,
Interface-Name/Vlan : L3-auth3/40,
User-Group : DST-GRP3,
Authentication-Type : IP,
Authentication-Status : Fail,
Session-Time Remaining(sec) : 200 sec

output definitions

UserName Displays either the IP address or Captive Portal user name for the learned user device.
IP-Address The IP address of the user device.
Destination IP-Network The destination IP network address for the user device.
Access Timestamp The date and time the user device accessed the network.
Interface-Name/VLAN The name of the IP interface and VLAN associated with the user device.
User-Group The name of the router authentication user group condition that matches the user device traffic.
Authentication-Type Indicates whether the user device attempted Captive Portal or IP-based authentication.
Authentication-Status Indicates whether the user device passed or failed authentication.
Session-Time Remaining (sec) The amount of time remaining for the users login session.

Release History
Release 8.5R4; command was introduced.

Related Commands

unp router-auth user flush Performs a MAC address flush of the specified router domain authentication users.

MIB Objects

N/A
**unp classification port**

Defines a Port classification rule for the specified UNP profile. If the UNP port or link aggregate on which the device traffic is received matches the port or link aggregate defined for the rule, the specified profile is applied to the device.

```
unp classification {port chassis/slot/port1|-port2] | linkagg [agg_id|-agg_id2]} [vlan-tag vlan_id | outer_vlan_id:inner_vlan_id] [profile1 profile_name [profile2 profile_name] [profile3 profile_name]]
```

```
no unp classification {port chassis/slot/port1|-port2] | linkagg agg_id} [profile1] [profile2] [profile3]
```

### Syntax Definitions

- `chassis/slot/port[-port2]`:
  The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).

- `[agg_id|-agg_id2]`:
  The link aggregate ID for a specific UNP link aggregate. Use a hyphen to specify a range of IDs (5-10).

- `vlan_id`:
  A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.

- `outer_vlan_id:inner_vlan_id`:
  An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.

- `profile_name`:
  The name of an existing UNP profile.

### Defaults

By default, no classification rules are defined for a UNP profile.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the Port rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.

- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

- The Port rule configured for the specified profile is applied only to traffic learned on the specified UNP port or link aggregate.

- If a range of ports is specified with this command, any non-UNP ports within the range are skipped.
When configuring a Port classification rule, specify an optional VLAN tag before specifying the UNP for which the rule will classify traffic.

Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:

- Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
- Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
- When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the matching traffic.

Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

If a VLAN ID tag is specified with this command, the UNP is applied only to tagged packets that are received on the specified UNP port and that contain the VLAN ID tag.

Untagged packets are only classified using the specified UNP port; the VLAN ID tag is ignored if it is specified with this rule.

A Port classification rule can be combined with a MAC address rule and IP address rule to configure a port-based binding rule.

**Examples**

```
-> unp classification port 1/1/5 vlan-tag 100 profile1 unp1-vxlan profile2 unp2-spb
-> unp classification port 1/1/10-15 profile1 unp1-vlan profile2 unp2-spb
-> no unp classification port 1/1/5 profile2
-> no unp classification port 1/1/5

-> unp classification linkagg 5 profile1 unp1-vlan profile2 unp2-vxlan profile3 unp3-spb
-> unp classification linkagg 6-10 vlan-tag 10:20 profile1 unp1-vlan
-> no unp classification linkagg 5 profile3
-> no unp classification linkagg 5
```

**Port + MAC address + IP address binding rule example:**

```
-> unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask 255.255.0.0 port 1/1/15 profile1 Pr3
-> no unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask 255.255.0.0 port 1/1/15
```

**Port + MAC address binding rule example:**

```
-> unp classification mac-address 00:11:22:33:44:55 port 1/1/5 profile1 Pr1
-> no unp classification mac-address 00:11:22:33:44:55 port 1/1/5
```

**Port + IP address binding rule example:**

```
-> unp classification ip-address 10.0.0.20 mask 255.255.0.0 port 1/1/10 profile1 Pr2
-> no unp classification ip-address 10.0.0.20 mask 255.255.0.0 port 1/1/10
```
**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp classification**: Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
- **unp profile**: Configures a UNP profile.
- **show unp classification**: Displays the UNP classification rule configuration.

**MIB Objects**

- alaDaUNPPortRuleTable
  - alaDaUNPPortRuleNum
  - alaDaUNPPortRuleVlanTag
  - alaDaUNPPortRuleProfile1
  - alaDaUNPPortRuleProfile2
  - alaDaUNPPortRuleProfile3
access guardian commands

unp classification domain

Defines a Domain ID classification rule for the specified UNP profile. If the port or link aggregate on which the device traffic is received belongs to a Domain ID that matches the Domain ID defined for the rule, the specified profile is applied to the device.

```
unp classification domain domain_id [vlan-tag vlan_id | outer_vlan_id:inner_vlan_id] {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}
no unp classification domain domain_id [profile1] [profile2] [profile3]
```

Syntax Definitions

- `domain_id` A domain ID number.
- `vlan_id` A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
- `outer_vlan_id:inner_vlan_id` An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
- `profile_name` The name of an existing UNP profile.

Defaults

By default, no classification rules are defined for a UNP profile.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to remove the domain ID rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring a Port classification rule, specify and optional VLAN tag before specifying the UNP for which the rule will classify traffic.
- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.

When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the matching traffic.

Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets received on a UNP port associated with the Domain ID and tagged with the specified VLAN ID.

Untagged packets are only classified using the specified domain ID; the VLAN ID tag is ignored if it is specified with this rule.

A domain ID classification rule can be combined with a MAC address rule and an IP address rule to configure a domain-based binding rule.

**Examples**

```
-> unp classification domain 10 profile1 unp1-vlan
-> unp classification domain 20 vlan-tag 100 profile1 unp1-vxlan profile2 unp2-spb profile3-vlan
-> no unp classification domain 20 profile3
-> no unp classification domain 20
```

Domain ID + MAC address + IP address binding rule example:

```
-> unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask 255.255.0.0 domain 10 profile1 Pr3
-> no unp classification mac-address 00:11:22:33:44:55 ip-address 10.0.0.20 mask 255.255.0.0 domain 10
```

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp classification**  Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
- **unp profile**  Configures a UNP profile.
- **show unp classification**  Displays the UNP classification rule configuration.

**MIB Objects**

- `alaDaUNPCustDomainRuleTable`
- `alaDaUNPCustDomainRuleId`
- `alaDaUNPCustDomainRuleVlanTag`
- `alaDaUNPCustDomainRuleProfile1`
- `alaDaUNPCustDomainRuleProfile2`
- `alaDaUNPCustDomainRuleProfile3`
**unp classification mac-address**

Defines a MAC address classification rule for the specified UNP. If the source MAC address of the device traffic matches the MAC address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

```
unp classification mac-address mac_address [domain domain_id] [vlan-tag vlan_id | outer_vlan_id:inner_vlan_id] [profile1 profile_name [profile2 profile_name] [profile3 profile_name]]
```

```
no unp classification mac-address mac_address [profile1] [profile2] [profile3]
```

### Syntax Definitions

- **mac_address**
  - MAC address (e.g., 00:00:39:59:f1:0c).

- **domain_id**
  - An existing customer domain ID to which this rule will apply.

- **vlan_id**
  - A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.

- **outer_vlan_id:inner_vlan_id**
  - An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.

- **profile_name**
  - The name of an existing UNP profile.

### Defaults

By default, no classification rules are defined for a UNP.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id</td>
<td>none</td>
</tr>
<tr>
<td>domain_id</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the MAC address rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.

- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
• When configuring a MAC address classification rule, specify and optional VLAN tag and/or an optional customer domain ID before specifying the UNP for which the rule will classify traffic.

• When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.

• Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  – Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  – Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  – When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the matching traffic.

• Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

• If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source MAC address and the VLAN ID tag.

• Untagged packets are only classified using the specified MAC address; the VLAN ID tag is ignored if it is configured for this rule.

Examples

-> unp classification mac-address 00:11:22:33:44:55 profile1 CustA
-> unp classification mac-address 00:2a:95:00:00:01 vlan-tag 200 profile1 VNP1
profile2 vxlp-1
-> unp classification mac-address 00:2b:96:11:22:03 profile1 CustA profile2 VNP1
profile3 vxlp-1
-> unp classification mac-address 00:11:22:33:44:56 domain 2 vlan-tag 100:200
profile1 CustB
-> unp classification mac-address 00:2a:95:00:00:02 domain 1 profile1 unp1-vlan
profile2 unp2-spb
-> no unp classification mac-address 00:2b:96:11:22:03 profile3
-> no unp classification mac-address 00:2a:95:00:00:02

Release History

Release 8.3.1; command introduced.
Related Commands

**unp classification** Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.

**unp domain** Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.

**unp profile** Configures a UNP profile.

**show unp classification** Displays the UNP classification rule configuration.

MIB Objects

alaDaUNPCustDomainMacRuleTable
  alaDaUNPCustDomainMacRuleDomainId
  alaDaUNPCustDomainMacRuleAddr
  alaDaUNPCustDomainMacRuleVlanTag
  alaDaUNPCustDomainMacRuleProfile1
  alaDaUNPCustDomainMacRuleProfile2
  alaDaUNPCustDomainMacRuleProfile3
**unp classification mac-oui**

Defines a MAC address Organizationally Unique Identifier (OUI) classification rule for the specified UNP profile. If the OUI of the source MAC address of the device traffic matches the OUI defined for the rule, the specified profile is applied to the device.

```
unp classification mac-oui mac_oui [vlan-tag vlan_id | outer_vlan_id:inner_vlan_id] {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}

no unp classification mac-oui mac_oui [profile1] [profile2] [profile3]
```

### Syntax Definitions

- **mac_oui**: The first three octets of the MAC address (for example, e8:39:35 is the OUI of MAC address e8:39:35:10:fe:11).
- **vlan_id**: A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
- **outer_vlan_id:inner_vlan_id**: An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
- **profile_name**: The name of an existing UNP profile.

### Defaults

By default, no classification rules are defined for a UNP.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the MAC OUI rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.
- When configuring a MAC address OUI classification rule, specify and optional VLAN tag before specifying the UNP for which the rule will classify traffic.
• Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  – Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  – Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  – When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the matching traffic.

• Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

• If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source MAC address OUI and the VLAN ID tag.

• Untagged packets are only classified using the specified MAC address OUI; the VLAN ID tag is ignored if it is specified with this rule.

Examples

-> unp classification mac-oui 00:11:22 profile1 unp1-vlan
-> unp classification mac-oui 00:11:33 vlan-tag 10 profile1 unp1-vlan profile2 unp2-spb profile3 unp3-vxlan
-> no classification mac-oui 00:11:33 profile3
-> no unp classification mac-oui 00:11:22

Release History

Release 8.3.1; command was introduced.

Related Commands

unp classification       Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp profile             Configures a UNP profile.
show unp classification  Displays the UNP classification rule configuration.

MIB Objects

alaDaUNPMacOuiRuleTable
alaDaUNPMacOuiRuleAddr
alaDaUNPMacOuiRuleVlanTag
alaDaUNPMacOuiRuleProfile1
alaDaUNPMacOuiRuleProfile2
alaDaUNPMacOuiRuleProfile3
**unp classification mac-range**

Defines a MAC address range classification rule for the specified UNP. If the source MAC address of the device traffic matches any address within the range of MAC addresses, the specified UNP is applied to the device. An optional VLAN ID tag parameter is also available to specify a VLAN tag that device traffic must also match in addition to the source MAC address.

```
unp classification mac-range low_mac_address high_mac_address [domain domain_id] [vlan-tag vlan_id | outer_vlan_id:inner_vlan_id] {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}
```

```
no unp classification mac-range low_mac_address high_mac_address [profile1] [profile2] [profile3]
```

### Syntax Definitions

- `low_mac_address`: MAC address that defines the low end of the range (e.g., 00:00:39:59:f1:00).
- `high_mac_address`: MAC address that defines the high end of the range (e.g., 00:00:39:59:f1:90).
- `domain_id`: An existing customer domain ID to which this rule will apply.
- `vlan_id`: A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.
- `outer_vlan_id:inner_vlan_id`: An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.
- `profile_name`: The name of an existing UNP profile.

### Defaults

By default, no classification rules are defined for a UNP.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>none</td>
</tr>
<tr>
<td><code>domain_id</code></td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the no form of this command to remove the MAC address range rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.

- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

- When configuring a MAC address range classification rule, specify and optional VLAN tag and/or an optional domain ID before specifying the UNP for which the rule will classify traffic.

- When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the matching traffic.

- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing a source MAC address within the specified range and the VLAN ID tag.

- Untagged packets are only classified using the specified MAC address range; the VLAN ID tag is ignored if it is specified with this rule.

Examples

-> unp classification mac-range 00:11:22:33:44:66 00:11:22:33:44:77 profile1 CustA
-> unp classification mac-range 00:11:22:33:44:99 00:11:22:33:45:01 vlan-tag 20 profile1 vNP1
-> unp classification mac-range 00:11:22:33:44:01 00:11:22:33:44:20 domain 2 profile1 CustB
-> unp classification mac-range 00:11:22:33:44:01 00:11:22:33:44:20 domain 3 vlan-tag 200 profile1 unp1-vlan profile2 unp2-spb profile3 unp3-vxlan

Release History

Release 8.3.1; command was introduced.
Related Commands

unp classification  Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.

unp domain  Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.

unp profile  Configures a UNP profile.

show unp classification  Displays the UNP classification rule configuration.

MIB Objects

alaDaUNPCustDomainMacRangeRuleTable
  alaDaUNPCustDomainMacRangeRuleLoAddr
  alaDaUNPCustDomainMacRangeRuleHiAddr
  alaDaUNPCustDomainMacRangeRuleVlanTag
  alaDaUNPCustDomainMacRangeRuleDomainId
  alaDaUNPCustDomainMacRangeRuleProfile1
  alaDaUNPCustDomainMacRangeRuleProfile2
  alaDaUNPCustDomainMacRangeRuleProfile3
unp classification ip-address

Defines an IP network address classification rule for the specified UNP. If the source IP address of the device traffic matches the IP address defined for the rule, the specified UNP is applied to the device. An optional VLAN ID tag parameter is available to specify a VLAN tag that device traffic must also match in addition to the source IP address.

```
unp classification ip-address ip_address mask subnet_mask [domain domain_id] [vlan-tag vlan_id | outer_vlan_id:inner_vlan_id] [profile1 profile_name [profile2 profile_name] [profile3 profile_name]]
```

```
no unp classification ip-address ip_address mask subnet_mask [profile1] [profile2] [profile3]
```

**Syntax Definitions**

- `ip_address` IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).

- `subnet_mask` An IP address mask to identify the IP subnet for the interface (supports class-less masking).

- `domain_id` An existing customer domain ID to which this rule will apply.

- `vlan_id` A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.

- `outer_vlan_id:inner_vlan_id` An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.

- `profile_name` The name of an existing UNP profile.

**Defaults**

By default, no classification rules are defined for a UNP.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>none</td>
</tr>
<tr>
<td><code>domain_id</code></td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

|                | 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 V72/C32 | 6900 X48C6/T48C6 | X48C4E/V48C8 | C32E/T24C2 | X24C2 | 9900 |
|----------------|------|------|------|-------|------|-------|------|------|---------------|------------------|----------------|-----------|-------|-------|------|
| supported      | Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes           | Yes              | Yes            | Yes       | Yes    | Yes   |      |

**Usage Guidelines**

- Use the `no` form of this command to remove an IP network address rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.
• Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

• When configuring an IP network address classification rule, specify and optional VLAN tag and/or an optional customer domain ID before specifying the UNP for which the rule will classify traffic.

• When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.

• Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  – Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  – Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  – When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the matching traffic.

• Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

• If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified source IP address and the VLAN ID tag.

• Untagged packets are only classified using the specified IP address; the VLAN ID tag is ignored if it is specified with this rule.

**Examples**

-> unp classification ip-address 10.1.1.1 mask 255.255.255.0 profile1 CustA
-> unp classification ip-address 20.1.1.1 mask 255.255.0.0 profile1 vNP1 profile2 vNP2
-> unp classification ip-address 50.1.1.1 mask 255.255.255.0 vlan-tag 300 profile1 CustB
-> unp classification ip-address 60.1.1.1 mask 255.255.0.0 domain 2 profile1 unp2 profile2 unp3-spb
-> unp classification ip-address 70.1.1.1 mask 255.255.0.0 domain 1 vlan-tag 20:30 profile1 vNP3
-> no unp classification ip-address 20.1.1.1 mask 255.255.0.0 profile2
-> no unp classification ip-address 10.1.1.1 mask 255.255.255.0

**Release History**

Release 8.3.1; command was introduced.
Related Commands

**unp classification**
Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.

**unp domain**
Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.

**unp profile**
Configures a UNP profile.

**show unp classification**
Displays the UNP classification rule configuration.

MIB Objects

alaDaUNPCustDomainIpNetRuleTable
- alaDaUNPCustDomainIpNetRuleDomainId
- alaDaUNPCustDomainIpNetRuleAddr
- alaDaUNPCustDomainIpNetRuleMask
- alaDaUNPCustDomainIpNetRuleVlanTag
- alaDaUNPCustDomainIpNetRuleProfile1
- alaDaUNPCustDomainIpNetRuleProfile2
- alaDaUNPCustDomainIpNetRuleProfile3
**unp classification vlan-tag**

Defines a VLAN tag classification rule for the specified UNP. If the VLAN ID tag of the device traffic matches the VLAN ID defined for the rule, the specified UNP is applied to the device.

```
unp classification vlan-tag {vlan_id | outer_vlan_id:inner_vlan_id} [domain domain_id] {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}
```

```
no unp classification vlan-tag vlan_id [profile1] [profile2] [profile3]
```

**Syntax Definitions**

- **vlan_id**
  A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.

- **outer_vlan_id:inner_vlan_id**
  An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.

- **domain_id**
  An existing customer domain ID to which this rule will apply.

- **profile_name**
  The name of an existing UNP profile.

**Defaults**

By default, no classification rules are defined for a UNP.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_id</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a VLAN tag rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.

- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

- When configuring a VLAN tag classification rule, specify an optional customer domain ID before specifying the name of the UNP for which the rule will classify traffic.
When a customer domain ID is configured for this rule, the rule is applied only to traffic received on UNP ports that are associated with the same domain ID. All UNP ports are automatically assigned to customer domain 0 at the time the port is configured as a UNP port.

Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:

- Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
- Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
- When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (Profile1 first, Profile2 second, and Profile3 third) to determine which profile is applied to the matching traffic.

Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

Untagged packets are not classified with this rule.

**Examples**

```
-> unp classification vlan-tag 400 profile1 CustA
-> unp classification vlan-tag 10:20 domain 3 profile1 unp1 profile2 spb1
-> no unp classification vlan-tag 10:20 profile1
-> no unp classification vlan-tag 400
```

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- **unp classification**  Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
- **unp domain**  Assigns a UNP port or link aggregate to the specified customer domain (UNP group) ID.
- **unp profile**  Configures a UNP profile.
- **show unp classification**  Displays the UNP classification rule configuration.

**MIB Objects**

- `alaDaUNPCustDomainVlanTagRuleTable`
- `alaDaUNPCustDomainVlanTagRuleDomainId`
- `alaDaUNPCustDomainVlanTagRuleVlan`
- `alaDaUNPCustDomainVlanTagRuleProfile1`
- `alaDaUNPCustDomainVlanTagRuleProfile2`
- `alaDaUNPCustDomainVlanTagRuleProfile3`
**unp classification lldp med-endpoint**

Defines a Link Layer Discovery Protocol (LLDP) classification rule for the specified UNP profile. This rule is used specifically for IP phones and OmniAccess Stellar Access Point (AP) devices.

```
unp classification lldp med-endpoint {ip-phone | access-point} {profile1 profile_name} {profile2 profile_name}] [profile3 profile_name]
```

```
no unp classification lldp med-endpoint {ip-phone | access-point} {profile1} {profile2} {profile3}
```

**Syntax Definitions**

- **ip-phone** When LLDP TLVs from an IP phone are detected, apply the specified profile to the IP phone.
- **access-point** When LLDP TLVs from an OmniAccess Stellar AP are detected, apply the specified profile to the AP device.
- **profile_name** The name of an existing UNP profile.

**Defaults**

By default, no classification rules are defined for a UNP profile.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.

- There is a built-in LLDP classification rule for access points that is assigned to built-in profiles named “defaultWLANProfile” and “defaultWLANAccessProfile”. This rule facilitates the automatic detection
and classification of OmniAccess Stellar APs that are connected to UNP bridge and access ports. Consider the following regarding the built-in LLDP access point rule:

- The rule cannot be removed from the switch configuration. However, the profile designation for the rule can be changed.
- The rule does not appear in the configuration snapshot for the switch unless the profile assignment for the rule was changed.
- When Stellar APs are detected on a UNP bridge port, they are classified and assigned to the VLAN that is mapped to the built-in “defaultWLANProfile”. This VLAN is advertised to the AP device as the management VLAN for untagged AP traffic.
- When Stellar APs are detected on a UNP access port, they are classified and assigned to the Shortest Path Bridging (SPB) service that is mapped to the built-in “defaultWLANAccessProfile”. This service is advertised to the AP device as the management service for untagged AP traffic.

- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (profile1 first, profile2 second, and profile3 third) to determine which profile is applied to the matching traffic.

- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

**Examples**

- `unp classification lldp med-endpoint ip-phone profile1 unp1-vlan profile2 unp2-vlan`
- `no unp classification lldp med-endpoint ip-phone profile2`
- `no unp classification lldp med-endpoint ip-phone`

- `unp classification lldp med-endpoint access-point profile1 defaultWLANProfile`
- `no unp classification lldp med-endpoint access-point`
- `unp classification lldp med-endpoint access-point`  
  ERROR: BUILT-IN Access-Point LLDP Rule cannot be deleted

**Release History**

Release 8.3.1; command was introduced.
Release 8.4.1.R02; **access-point** parameter added.
Related Commands

**unp classification**  Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.

**unp profile**  Configures a UNP profile.

**show unp classification**  Displays the UNP classification rule configuration.

MIB Objects

alaDaUNPEndPoinRuleTable  
alaDaUNPEndPoinRuleId  
alaDaUNPEndPoinProfile1  
alaDaUNPEndPoinProfile2  
alaDaUNPEndPoinProfile3
**unp classification authentication-type**

Defines an Authentication Type classification rule for the specified UNP profile. If the type of authentication applied to the device traffic matches the authentication type defined for the rule, the specified profile is applied to the device.

```
unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [vlan-tag vlan_id]
outer_vlan_id:inner_vlan_id {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}
```

```
no unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [profile1 profile2 profile3]
```

### Syntax Definitions

- **none**
  - No authentication was applied to the device.

- **mac**
  - The device was successfully authenticated through MAC authentication.

- **802.1x**
  - The device was successfully authenticated through 802.1X authentication.

- **fail**
  - Optional parameter to specify failed MAC or 802.1X authentication.

- **vlan_id**
  - A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets.

- **outer_vlan_id:inner_vlan_id**
  - An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.

- **profile_name**
  - The name of an existing UNP profile.

### Defaults

By default, no classification rules are defined for a UNP profile.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the **no** form of this command to remove the rule or one or more of the associated profiles. When a classification rule is removed or modified, all MAC addresses classified with that rule are flushed.

- The optional **fail** parameter is used only in combination with the **mac** or **802.1x** parameter. When configured, the device is checked for a failed MAC or 802.1X authentication condition to determine whether or not the profile is applied.

- When the **fail** parameter is not specified (the default), the device is checked for a successful MAC or 802.1X authentication condition to determine whether or not the profile is applied.

- Adding a UNP classification rule to the switch configuration does not cause a MAC address flush.

- When configuring this type of classification rule, specify an optional VLAN tag before specifying the UNP profile name for which the rule will classify traffic.

- Up to three different profile names are configurable for a classification rule. The profile applied to matching traffic is based on the order of precedence and mapping of each profile. For example:
  - Profiles mapped to a VLAN are applied only to matching traffic received on UNP bridge ports.
  - Profiles mapped to a service (SPB, VXLAN, or static) are only applied to matching traffic received on UNP access ports.
  - When a classification rule is configured with multiple profiles and traffic received on a UNP port matches the rule, each profile is checked in the order of precedence (**profile1** first, **profile2** second, and **profile3** third) to determine which profile is applied to the matching traffic.

- Configuring both a VLAN profile and a service profile for the same rule ensures that the rule will be applied to traffic received on both types of UNP ports (bridge and access).

- If a VLAN ID tag is specified with this command, the UNP is only applied to tagged packets containing the specified authentication type *and* the VLAN ID tag.

- Untagged packets are only classified using the specified authentication type; the VLAN ID tag is ignored if it is specified with this rule.

Examples

```plaintext
-> unp classification authentication-type 802.1X profile1 unp1-vlan profile2 unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type 802.1X profile2
-> no unp classification authentication-type 802.1X

-> unp classification authentication-type 802.1X fail profile1 unp1-vlan profile2 unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type 802.1X fail profile3
-> no unp classification authentication-type 802.1X fail

-> unp classification authentication-type MAC profile1 unp1-vlan profile2 unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type MAC profile2
-> no unp classification authentication-type MAC

-> unp classification authentication-type MAC fail profile1 unp1-vlan profile2 unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type MAC fail profile3
-> no unp classification authentication-type MAC fail

-> unp classification authentication-type MAC vlan-tag 10 profile1 unp1-vlan
```
profile2 unp2-vlan profile3 unp3-vlan
-> no unp classification authentication-type MAC profile2
-> no unp classification authentication-type MAC

Release History
Release 8.3.1; command was introduced.

Related Commands
unp classification Configures the classification status for the UNP port. Rules are not applied when classification is disabled for the port.
unp profile Configures a UNP profile.
show unp classification Displays the UNP classification rule configuration.

MIB Objects
alaDaUNPAuthRuleTable
alaDaUNPAuthRuleType
alaDaUNPAuthRuleVlanTag
alaDaUNPAuthRuleProfile1
alaDaUNPAuthRuleProfile2
alaDaUNPAuthRuleProfile3
**unp classification-rule**

Configures an extended classification rule name and assigns a precedence value to the specified name. This type of rule defines a list of rule conditions, all of which a device must match to be classified into the UNP profile associated with the extended rule name.

```
unp classification-rule rule_name [precedence precedence_value] [profile1 profile_name] [profile2 profile_name] [profile3 profile_name]
```

```
no unp classification-rule rule_name [profile1] [profile2] [profile3]
```

### Syntax Definitions

- **rule_name**
  - The name to associate with the extended classification rule.

- **precedence_value**
  - The precedence level to assign to the extended rule. The valid range is 1–255 (1 = lowest, 255 = highest). Precedence value 255 is reserved for Device Profiling classification rules.

- **profile_name**
  - The name of an existing UNP profile to assign to the extended rule.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>precedence_value</td>
<td>1</td>
</tr>
<tr>
<td>profile_name</td>
<td>none</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the extended rule from the switch configuration or to remove a UNP profile name assigned to the rule.

- The precedence value specified with this command is used to determine precedence among extended classification rules.

- Extended rules take precedence over all other UNP classification rules (individual rules and binding rule combinations).

- Although some individual classification rules can be combined to form a binding rule, a binding rule is not assigned a rule name and does not have a configurable precedence value. In addition, extended classification rules offer more rule combinations than binding rules.
The following extended classification rules are automatically defined when Device Profiling is enabled for the switch (these rules cannot be removed):

- devProfPrinter
- devProfWindows
- devProfIP-Phone
- devProfWireless-Router
- devProfSmartPhone/PDA/Tablets

**Examples**

- `-> unp classification-rule ext-r1`
- `-> unp classification-rule ext-r1 profile1 UNP1 profile2 UNP2`
- `-> unp classification-rule ext-r1 precedence 250`

- `-> unp classification-rule ext-r2`
- `-> unp classification-rule ext-r2 precedence 255`
ERROR: Precedence 255 is reserved for Device Profiling
- `-> unp classification-rule ext-r2 precedence 254`
- `-> unp classification-rule ext-r2 profile1 UNP3 profile2 UNP4 profile3 UNP5`

- `-> no unp classification-rule ext-r1 profile1 UNP1`
- `-> no unp classification-rule ext-r1`

- `-> no unp classification-rule ext-r2 profile1 UNP4`
- `-> no unp classification-rule ext-r2`

- `-> no unp classification-rule devProfPrinter`
ERROR: Device Profiling Rule cannot be modified

**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; **edge-profile** parameter deprecated; **profile1**, **profile2**, and **profile3** parameters added.
Release 8.5R2; precedence value 255 reserved for Device Profiling extended classification rules.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>unp classification-rule port</code></td>
<td>Defines a Port rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule domain</code></td>
<td>Defines a Group ID rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule mac-address</code></td>
<td>Defines a MAC address rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule mac-oui</code></td>
<td>Defines a MAC OUI rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule mac-range</code></td>
<td>Defines a MAC address range rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule ip-address</code></td>
<td>Defines an IP address rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule vlan-tag</code></td>
<td>Defines a VLAN tag rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule lldp med-endpoint</code></td>
<td>Defines an LLDP endpoint rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule authentication-type</code></td>
<td>Defines an authentication type rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp classification-rule device-type</code></td>
<td>Defines a Device Profiling rule condition for an extended classification rule.</td>
</tr>
<tr>
<td><code>unp profile</code></td>
<td>Configures a UNP profile.</td>
</tr>
<tr>
<td><code>unp classification</code></td>
<td>Configures the classification status for the UNP port. Rules are not applied when the port classification status is disabled.</td>
</tr>
<tr>
<td><code>show unp classification-rule</code></td>
<td>Displays the UNP extended classification rule configuration.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- alaDaUNPClassifRuleTable
- alaDaUNPClassifRuleName
- alaDaUNPClassifRulePrecedenceNum
- alaDaUNPClassifRuleProfile1
- alaDaUNPClassifRuleProfile2
- alaDaUNPClassifRuleProfile3
unp classification-rule port

Defines a Port rule condition for the specified extended classification rule name.

unp classification-rule rule_name {port chassis/slot/port1[-port2] | linkagg agg_id}

no unp classification-rule rule_name {port | linkagg}

**Syntax Definitions**

- **rule_name**
  - The name of an extended classification rule to which the rule condition is assigned.

- **chassis/slot/port1[-port2]**
  - The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).

- **agg_id**
  - Link aggregate ID.

**Defaults**

By default, no conditions are defined when an extended classification rule is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the no form of this command to remove the Port rule condition from the specified extended classification rule name.

- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

**Examples**

- `unp classification-rule ext-r1 port 1/1/10`
- `no unp classification-rule ext-r1 port`

- `unp classification-rule ext-r2 port 1/1/1-5`
- `no unp classification-rule ext-r2 port`

- `unp classification-rule ext-r3 linkagg 10`
- `unp classification-rule ext-r3 linkagg`
**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `unp classification-rule`  
  Configures an extended classification rule name and associated profile.

- `show unp classification-rule`  
  Displays the UNP extended classification rule configuration.

**MIB Objects**

- `alaDaUNPClassifRuleTable`  
- `alaDaUNPClassifRuleName`  
- `alaDaUNPClassifRulePort`
unp classification-rule domain

Defines a domain ID rule condition for the specified extended classification rule name.

```
unp classification-rule rule_name domain domain_id
no unp classification-rule rule_name domain
```

### Syntax Definitions

- `rule_name`: The name of an extended classification rule to which the rule condition is assigned.
- `domain_id`: Domain ID number.

### Defaults

By default, no conditions are defined when an extended classification rule is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the Domain ID rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

### Examples

```
-> unp classification-rule ext-r1 domain-id GRP1
-> no unp classification-rule ext-r1 domain-id
```

### Release History

- Release 8.1.1; command was introduced.
- Release 8.3.1; `group-id` parameter changed to `domain`. 
Related Commands

**unp classification-rule**  
Configures an extended classification rule name and associated profile.

**show unp classification-rule**  
Displays the UNP extended classification rule configuration.

MIB Objects

alaDaUNPClassifRuleTable
alaDaUNPClassifRuleName
alaDaUNPClassifRuleCustomerDomain
**unp classification-rule mac-address**

Defines a MAC address, rule condition for the specified extended classification rule name.

**unp classification-rule** *rule_name* mac-address *mac_address*

**no unp classification-rule** *rule_name* mac-address

**Syntax Definitions**

- **rule_name**: The name of an extended classification rule to which the rule condition is assigned.
- **mac_address**: MAC address (e.g., 00:00:39:59:f1:0c).

**Defaults**

By default, no conditions are defined when an extended classification rule is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- Configuring all three types of MAC rules (MAC address, MAC OUI, and MAC address range) for the same extended classification rule is not allowed. Only one type of MAC rule is configurable for a given extended classification rule.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

**Examples**

- `-> unp classification-rule ext-r1 mac-address 00:11:22:33:44:55`
- `-> no unp classification-rule ext-r1 mac-address`

**Release History**

Release 8.1.1; command was introduced.
Related Commands

**unp classification-rule**  
Configures an extended classification rule name and associated UNP profile.

**show unp classification-rule**  
Displays the UNP extended classification rule configuration.

MIB Objects

- alaDaUNPClassifRuleTable
- alaDaUNPClassifRuleName
- alaDaUNPClassifRuleMacAddr
**unp classification-rule mac-oui**

Defines a MAC OUI rule condition for the specified extended classification rule name.

```
unp classification-rule rule_name mac-oui mac_oui
no unp classification-rule rule_name mac-oui
```

### Syntax Definitions

- **rule_name**: The name of an extended classification rule to which the rule condition is assigned.
- **mac_address**: MAC address (e.g., 00:00:39:59:f1:0c).
- **mac_oui**: The Organizationally Unique Identifier (OUI) of the MAC address. The OUI is the first three octets of the MAC address (for example, e8:39:35 is the OUI of MAC address e8:39:35:10:fe:11).

### Defaults

By default, no conditions are defined when an extended classification rule is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the rule condition from the specified extended classification rule name.
- Configuring all three types of MAC rules (MAC address, MAC OUI, and MAC address range) for the same extended classification rule is not allowed. Only one type of MAC rule is configurable for a given extended classification rule.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

### Examples

```
-> unp classification-rule ext-r1 mac-oui 00:11:22
-> no unp classification-rule ext-r1 mac-oui
```

### Release History

Release 8.1.1; command was introduced.
Related Commands

unp classification-rule  Configures an extended classification rule name and associated profile.
show unp classification-rule  Displays the UNP extended classification rule configuration.

MIB Objects

alaDaUNPClassifRuleTable
alaDaUNPClassifRuleName
alaDaUNPClassifRuleMacOuiAddr
unp classification-rule mac-range

Defines a MAC address range rule condition for the specified extended classification rule name.

unp classification-rule rule_name mac-range low_mac_address high_mac_address

no unp classification-rule rule_name mac-range

Syntax Definitions

rule_name The name of an extended classification rule to which the rule condition is assigned.

low_mac_address MAC address that defines the low end of the range (for example, 00:00:39:59:f1:00).

high_mac_address MAC address that defines the high end of the range (for example, 00:00:39:59:f1:90).

Defaults

By default, no conditions are defined when an extended classification rule is created.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the rule condition from the specified extended classification rule name.

- Configuring all three types of MAC rules (MAC address, MAC OUI, and MAC address range) for the same extended classification rule is not allowed. Only one type of MAC rule is configurable for a given extended classification rule.

- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

Examples

- no unp classification-rule ext-r1 mac-range

Release History

Release 8.1.1; command was introduced.
Related Commands

- **unp classification-rule** Configures an extended classification rule name and associated profile.
- **show unp classification-rule** Displays the UNP extended classification rule configuration.

MIB Objects

- `alaDaUNPClassifRuleTable`
- `alaDaUNPClassifRuleName`
- `alaDaUNPClassifRuleMacRngLoaddr`
- `alaDaUNPClassifRuleMacRngHiaddr`
unp classification-rule ip-address

Defines an IP network address rule condition for the specified extended classification rule name.

```plaintext
unp classification-rule rule_name ip-address ip_address mask subnet_mask
no unp classification-rule rule_name ip-address
```

**Syntax Definitions**

- **rule_name**: The name of an extended classification rule to which the rule condition is assigned.
- **ip_address**: IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).
- **subnet_mask**: An IP address mask to identify the IP subnet for the interface (supports class-less masking).

**Defaults**

By default, no conditions are defined when an extended classification rule is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

**Examples**

```
-> unp classification-rule ext-r1 ip-address 10.0.0.20 mask 255.0.0.0
-> no unp classification-rule ext-r1 ip-address
```

**Release History**

Release 8.1.1; command was introduced.
Related Commands

unp classification-rule Configures an extended classification rule name and associated profile.
show unp classification-rule Displays the UNP extended classification rule configuration.

MIB Objects

alaDaUNPClassifRuleTable
alaDaUNPClassifRuleName
alaDaUNPClassifRuleIpAddrType
alaDaUNPClassifRuleIpAddr
alaDaUNPClassifRuleIpMaskType
alaDaUNPClassifRuleIpMask
unp classification-rule vlan-tag

Defines a VLAN tag rule condition for the specified extended classification rule name.

```
unp classification-rule rule_name vlan-tag [vlan_id | outer_vlan_id:inner_vlan_id]
no unp classification-rule vlan-tag
```

**Syntax Definitions**

- **rule_name**: The name of an extended classification rule to which the rule condition is assigned.
- **vlan_id**: A VLAN ID to match single-tagged packets or the outer VLAN tag of double-tagged packets. Specify a value of zero to classify untagged traffic.
- **outer_vlan_id:inner_vlan_id**: An outer VLAN ID and an inner VLAN ID to match double-tagged packets. For example, 10:20 specifies that only packets with an outer tag of 10 and an inner tag of 20 will match this rule.

**Defaults**

By default, no conditions are defined when an extended classification rule is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

**Examples**

- `-> unp classification-rule ext-r1 vlan-tag 200`
- `-> unp classification-rule ext-r2 vlan-tag 10:20`
- `-> unp classification-rule ext-r3 vlan-tag 0`
- `-> no unp classification-rule ext-r1 vlan-tag`

**Release History**

Release 8.2.1; command was introduced.
**Related Commands**

- `unp classification-rule` Configures an extended classification rule name and associated profile.
- `show unp classification-rule` Displays the UNP extended classification rule configuration.

**MIB Objects**

- `alaDaUNPClassifRuleTable`
  - `alaDaUNPClassifRuleName`
  - `alaDaUNPClassifRuleVlanTag`
unp classification-rule lldp med-endpoint

Defines an LLDP rule condition for the specified extended classification rule name. This rule condition is specifically to detect IP phone TLVs or OmniAccess Stellar Access Point (AP) TLVs.

```
unp classification-rule rule_name lldp med-endpoint {ip-phone | access-point}
no unp classification-rule rule_name lldp med-endpoint ip-phone
```

### Syntax Definitions

- **rule_name**: The name of an extended classification rule to which the port condition is assigned.
- **ip-phone**: When LLDP TLVs from an IP phone are detected, apply the specified profile to the IP phone.
- **access-point**: When LLDP TLVs from an OmniAccess Stellar AP are detected, apply the specified profile to the AP device.

### Defaults

By default, no conditions are defined when an extended classification rule is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the rule condition from the specified extended classification rule name.
- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.
- When using the `access-point` option to define this rule condition, make sure “defaultWLANProfile” is assigned as the profile for the specified extended classification rule name.

### Examples

```
-> unp classification-rule ext-r1 lldp med-endpoint ip-phone
-> no unp classification-rule ext-r1 lldp med-endpoint ip-phone

-> unp classification-rule AP profile1 defaultWLANProfile
-> unp classification-rule AP lldp med-endpoint access-point
-> no unp classification-rule AP lldp med-endpoint access-point
```
**Release History**

Release 8.1.1; command was introduced.
Release 8.4.1.R02; **access-point** parameter added.

**Related Commands**

- **unp classification-rule** Configures an extended classification rule name and associated profile.
- **show unp classification-rule** Displays the UNP extended classification rule configuration.

**MIB Objects**

- alaDaUNPClassifRuleTable
- alaDaUNPClassifRuleName
- alaDaUNPClassifRuleEndPoin
**unp classification-rule authentication-type**

Defines an authentication type rule condition for the specified extended classification rule name.

```
unp classification-rule rule_name authentication-type {none | mac [fail] | 802.1x [fail]}
no unp classification-rule rule_name authentication-type
```

**Syntax Definitions**

- `rule_name` - The name of an extended classification rule to which the port condition is assigned.
- `none` - No authentication was applied to the device.
- `mac` - The device was successfully authenticated through MAC authentication.
- `802.1x` - The device was successfully authenticated through 802.1X authentication.
- `fail` - Optional parameter to specify failed MAC or 802.1X authentication.

**Defaults**

By default, no conditions are defined when an extended classification rule is created.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the rule condition from the specified extended classification rule name.

- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

- The optional `fail` parameter is used only in combination with the `mac` or `802.1x` parameter. When configured, the device is checked for a failed MAC or 802.1X authentication condition to determine whether or not the profile is applied.

- When the `fail` parameter is not specified (the default), the device is checked for a successful MAC or 802.1X authentication condition to determine whether or not the profile is applied.

**Examples**

```
-> unp classification-rule ext-r1 authentication-type 8021x
-> unp classification-rule ext-r1 authentication-type 8021X fail
```
Access Guardian Commands

unp classification-rule authentication-type

-> unp classification-rule ext-r1 authentication-type mac
-> unp classification-rule ext-r1 authentication-type mac fail
-> no unp classification-rule ext-r1 authentication-type

Release History
Release 8.1.1; command was introduced.

Related Commands
unp classification-rule Configures an extended classification rule name and associated profile.
show unp classification-rule Displays the UNP extended classification rule configuration.

MIB Objects
alaDaUNPClassifRuleTable
alaDaUNPClassifRuleName
alaDaUNPClassifRuleAuthType
unp classification-rule device-type

Defines a Device Profiling rule condition for the specified extended classification rule name.

```
unp classification-rule rule_name device-type device_name
no unp classification-rule rule_name device-type
```

### Syntax Definitions

- **rule_name**: The name of an extended classification rule to which the rule condition is assigned.
- **device_name**: The name of a device type to which the condition is assigned.

### Defaults

By default, no conditions are defined when an extended classification rule is created.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the rule condition from the specified extended classification rule name.

- If the extended classification rule name specified with this command does not exist, the switch will automatically create the extended rule name and associate the port rule condition with that name.

- The following extended classification rules are automatically defined when Device Profiling is enabled for the switch (the device type for these rules cannot be removed):
  - devProfPrinter
  - devProfWindows
  - devProfIP-Phone
  - devProfWireless-Router
  - devProfSmartPhone/PDA/Tablets

### Examples

```
-> unp classification-rule ext-rl device-type Printer
-> no unp classification-rule ext-rl device-type
-> no unp classification-rule devProfPrinter device-type
```
ERROR: Device-type cannot be modified on built-in rules

**Release History**

Release 8.5R2; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp classification-rule</td>
<td>Configures an extended classification rule name and associated profile.</td>
</tr>
<tr>
<td>show unp classification-rule</td>
<td>Displays the UNP extended classification rule configuration.</td>
</tr>
</tbody>
</table>

**MIB Objects**

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aDaUNPClassifRuleTable</td>
<td></td>
</tr>
<tr>
<td>aDaUNPClassifRuleName</td>
<td></td>
</tr>
<tr>
<td>aDaUNPClassifRuleDeviceType</td>
<td></td>
</tr>
</tbody>
</table>
**unp user-role**

Configures a user-defined role name and assigns a precedence value to the specified name. This type of role is used to define a list of conditions and a QoS policy list name. If the current context of a device matches all of the role conditions, then the policy list is applied to that device.

```
unp user-role role_name [precedence precedence_value]

no unp user-role role_name
```

**Syntax Definitions**

- `role_name` The name to associate with the user-defined role.
- `precedence_value` The precedence level to assign to the user-defined role. The valid range is 1–255 (1 = lowest, 255 = highest).

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>precedence_value</td>
<td>1</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the user-defined role from the switch configuration.
- The precedence value specified with this command is used to determine precedence among other user-defined roles.
- Every time the user context changes for a device, all the user-defined roles are checked to see if there is a role that matches the current user context.
- Only one user-defined role per user is allowed because only one QoS policy list per user is allowed.

**Examples**

```
-> unp user-role role1
-> unp user-role role2 precedence 255
-> no unp user-role role2
```
Release History

Release 8.1.1; command was introduced.

Related Commands

unp user-role policy-list
Assigns a QoS policy list to a user-defined role.

unp user-role profile
Configures a UNP profile condition for a user-defined role name.

unp user-role authentication-type
Defines an authentication type condition for a user-defined role name.

unp user-role cp-status-post-login
Configures the Captive Portal post login status as a condition for a user-defined role.

show unp user-role
Displays the user-defined role configuration for the switch.

MIB Objects

alaDaUNPUserRoleTable
alaDaUNPUserRoleName
alaDaUNPUserRolePrecedenceNum
**unp user-role policy-list**

Assigns a QoS policy list to the specified user-defined role name. When the context of a user device matches all the user-defined role conditions, the policy list associated with the role is applied to the device.

`unp user-role role_name policy-list list_name`

`no unp user-role role_name policy-list`

---

**Syntax Definitions**

- `role_name`: The name of a user-defined role to which the QoS policy list is assigned.
- `list_name`: The name of an existing QoS policy list.

---

**Defaults**

By default, no QoS policy list is assigned to a user-defined role.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to remove a QoS policy list from the specified user-defined role.
- If the user-defined role name specified with this command does not exist, the switch will automatically create the role name and associate the QoS policy list with that name.
- The QoS policy list name specified with this command must already exist in the switch configuration.

---

**Examples**

- -> unp user-role role1 policy-list role1-list
- -> unp user-role role2 policy-list role2-list
- -> no unp user-role role2 policy-list

---

**Release History**

Release 8.1.1; command was introduced.
Related Commands

unp user-role Configures the name and precedence for a user-defined role.
policy list Configures a QoS policy list.
show unp user-role Displays the user-defined role configuration for the switch.

MIB Objects

alaDaUNPUserRoleTable
alaDaUNPUserRoleName
alaDaUNPUserRolePolicyList
**unp user-role profile**

Defines a UNP profile condition for the specified user-defined role name.

```
unp user-role role_name {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}
no unp user-role role_name [profile1] [profile2] [profile3]
```

**Syntax Definitions**

- `role_name` The name of a user-defined role.
- `profile_name` The name of an existing UNP profile.

**Defaults**

By default, the profile condition is not configured for a user-defined role.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the profile name as a condition for the specified user-defined role.
- If the user-defined role name specified with this command does not exist, the switch will automatically create the role name and associate the profile with that name.
- The profile name specified with this command must already exist in the switch configuration.

**Examples**

```
-> unp user-role role1 profile1 unp1
-> unp user-role role2 profile1 unp1 profile2 unp2
-> unp user-role role3 profile1 unp1 profile2 unp2 profile3 unp3
-> no unp user-role role1 profile1
-> no unp user-role role2 profile1 profile2
-> no unp user-role role3 profile3
```

**Release History**

Release 8.1.1; command was introduced.
**Related Commands**

- **unp user-role**
  Configures the name and precedence for a user-defined role.

- **unp user-role policy-list**
  Assigns a QoS policy list to a user-defined role.

- **show unp user-role**
  Displays the user-defined role configuration for the switch.

**MIB Objects**

- alaDaUNPUserRoleTable
- alaDaUNPUserRoleName
- alaDaUNPUserRoleProfile1
- alaDaUNPUserRoleProfile2
- alaDaUNPUserRoleProfile3
unp user-role authentication-type

Defines an authentication type condition for the specified user-defined role name.

```
unp user-role role_name authentication-type {none | mac [fail] | 802.1x [fail]}
```

```
no unp user-role role_name authentication-type
```

**Syntax Definitions**

- **role_name**: The name of a user-defined role.
- **none**: No authentication was applied to the device.
- **mac**: The device was successfully authenticated through MAC authentication.
- **802.1x**: The device was successfully authenticated through 802.1X authentication.
- **fail**: Optional parameter to specify failed MAC or 802.1X authentication.

**Defaults**

By default, the authentication type condition is not configured for a user-defined role.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the authentication type as a condition for the specified user-defined role.

- If the user-defined role name specified with this command does not exist, the switch will automatically create the role name and associate the profile with that name.

- The optional `fail` parameter is used only in combination with the `mac` or `802.1x` parameter. When configured, the device is checked for a failed MAC or 802.1X authentication condition to determine whether or not the user role (policy list associated with the user role) is applied to the device.

- When the `fail` parameter is not specified (the default), the device is checked for a successful MAC or 802.1X authentication condition to determine whether or not the user role (policy list associated with the user role) is applied to the device.

**Examples**

```
-> unp user-role role1 authentication-type 8021x
-> unp user-role role1 authentication-type 8021X fail
```
Access Guardian Commands

unp user-role authentication-type

-> unp user-role role1 authentication-type mac
-> unp user-role role1 authentication-type mac fail
-> no unp user-role role1 authentication-type

Release History

Release 8.1.1; command was introduced.

Related Commands

unp user-role  
Configures the name and precedence for a user-defined role.

unp user-role policy-list  
Assigns a QoS policy list to a user-defined role.

show unp user-role  
Displays the user-defined role configuration for the switch.

MIB Objects

alaDaUNPUserRoleTable
alaDaUNP UserRoleName
alaDaUNP UserRole AuthType
**unp user-role cp-status-post-login**

Configures the Captive Portal (CP) post login status as a condition for the specified user-defined role name.

```plaintext
unp user-role role_name cp-status-post-login
no unp user-role role_name cp-status-post-login
```

**Syntax Definitions**

`role_name` The name of an existing user-defined role.

**Defaults**

By default, the CP post login status condition is not configured for a user-defined role.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the CP post login status as a condition for the specified user-defined role.
- When this condition is active for a user-defined role, the switch will check to see if a device is in a CP post login state before applying the QoS policy list associated with the user-defined role.

**Examples**

```plaintext
-> unp user-role role1 cp-status-post-login
-> no unp user-role role1 cp-status-post-login
```

**Release History**

Release 8.1.1; command was introduced.
Related Commands

- **unp user-role**  Confirms the name and precedence for a user-defined role.
- **unp user-role policy-list**  Assigns a QoS policy list to a user-defined role.
- **show unp user-role**  Displays the user-defined role configuration for the switch.

MIB Objects

- alaDaUNPUserRoleTable
- alaDaUNPUserRoleName
- alaDaUNPUserRolePostLoginStatus
**unp restricted-role policy-list**

Assigns an explicit QoS policy list to an implicit restricted role. When the switch assigns a user device to one of the restricted role states (unauthorized, Quarantine Manager, or Captive Portal pre-login), the explicit QoS policy list is applied instead of the built-in policy list associated with the restricted role.

```
unp restricted-role {unauthorized | qmr | cp-prelogin} policy-list list_name
```

```
nounp restricted-role {unauthorized | qmr | cp-prelogin} policy-list
```

**Syntax Definitions**

- `list_name`: The name of an existing QoS policy list.
- `unauthorized`: Applies the explicit policy list to unauthorized devices.
- `qmr`: Applies the explicit policy list to quarantined devices. *Not supported on the OmniSwitch 6360.*
- `cp-prelogin`: Applies the explicit policy list to devices in a Captive Portal pre-login state.

**Defaults**

By default, the built-in policy list associated with the restricted role state.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the explicit QoS policy list assignment.
- An explicit QoS policy list overrides the built-in policy list associated with the restricted role state.
- When the explicit policy list assignment is removed, the switch reverts back to using the built-in policy list associated with the restricted role state.

**Examples**

- `unp restricted-role unauthorized policy-list unauth1`
- `unp restricted-role qmr policy-list quarantined1`
- `unp restricted-role cp-prelogin policy-list cplogin1`
- `no unp restricted-role unauthorized`
- `no unp restricted-role qmr`
- `no unp restricted-role cp-prelogin`
**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- **policy list**
  - Configures a QoS policy list.

- **show unp restricted-role**
  - Displays the UNP restricted role policy list configuration.

**MIB Objects**

- alaDaUNPRstrctedRoleTable
- alaDaUNPRstrctedRoleType
- alaDaUNPRstrctedRolePolicyList
captive-portal mode

Configures the Captive Portal mode of operation.

captive-portal mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}

no captive-portal mode internal

**Syntax Definitions**

- **internal** Internal Captive Portal (Web server is on the switch. A VLAN change requires a port bounce).
- **internal dhcp** Internal DHCP Captive Portal (Web server is on the switch. IP address from Captive Portal subnet is leased to the client; VLAN change does not require a port bounce).
- **ip-lease-time seconds** The amount of time an IP address is leased to a client. The valid range is 20–120 seconds.
- **ip-renew-time seconds** The amount of time until a client with a leased IP address attempts to renew the leased IP address.
- **ip-rebinding-time seconds** The amount of time until a client attempts to obtain a new leased IP address (occurs when renew attempts fail).
- **external** Not supported; an external Captive Portal operation is provided through the OmniSwitch Bring Your Own Device (BYOD) solution.

**Defaults**

By default, the mode is set to internal Captive Portal. When the internal DHCP Captive Portal mode is selected without specifying any optional parameter values, the following default values are set:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-lease-time</td>
<td>30 seconds</td>
</tr>
<tr>
<td>ip-renew-time</td>
<td>15 seconds</td>
</tr>
<tr>
<td>ip-rebinding-time</td>
<td>26 seconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- Use the `no` form of this command to revert the Captive Portal mode back to the default internal mode (no internal DHCP functionality).

- Only the internal and internal DHCP Captive Portal modes (Web server on the switch) are configurable for the switch. An external Captive Portal operation is provided through interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch BYOD solution.

- When a device is classified into a UNP profile that has the Captive Portal authentication attribute enabled, the device is placed into a Captive Portal pre-login state. The Captive Portal mode determines how a device in the pre-login state obtains an IP address, the necessary DNS information, and whether a port bounce is required after a VLAN change.
  
  - If the internal Captive Portal mode (the default) is active, the device can directly contact a DHCP server to get an IP address and DNS information. A port bounce action is required if the initial VLAN assignment for the device is changed.
  
  - If the internal DHCP Captive Portal mode is active, the switch provides basic DHCP functionality to assign the device an IP address with a short-term lease from the Captive Portal subnet (10.123.0.0) and provide the necessary DNS information. A port bounce action is not required if the initial VLAN assignment for the device is changed.

- Consider the following when changing the internal DHCP parameter values:
  
  - The `ip-renew-time` is 50% of the `ip-lease-time`.
  
  - The `ip-rebinding-time` is 87.5% of the `ip-lease-time`.
  
  - When only the `ip-lease-time` is changed, the `ip-renew-time` and `ip-rebinding-time` are automatically recalculated based on the noted percentages.
  
  - Make sure the `ip-renew-time` specified is less than the `ip-rebinding-time`.
  
  - Make sure the `ip-rebinding-time` specified falls between the `ip-renew-time` and `ip-lease-time`.

**Examples**

```plaintext
-> captive-portal mode internal-dhcp
-> captive-portal mode internal-dhcp ip-least-time 120
-> captive-portal mode internal
-> no captive-portal mode internal
```

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- `show captive-portal configuration`

  Displays the global Captive Portal configuration for the switch.

**MIB Objects**

- `alaDaCPortalGlobalConfig`
- `alaDaCPortalMode`
- `alaDaCPortalDHCPLeaseTime`
- `alaDaCPortalDHCPRenewTime`
- `alaDaCPortalDHCPRebindingTime`
captive-portal name

Configures an IP address or Fully Qualified Domain Name (FQDN) as a redirect URL to use for Captive Portal.

`captive-portal name {ip_address | domain_name}`

`no captive-portal name`

**Syntax Definitions**

- `ip_address` The IPv4 network address (e.g., 171.15.0.0) to which HTTP traffic is redirected.
- `domain_name` An FQDN (up to 32 characters) to which HTTP traffic is redirected.

**Defaults**

By default, the Captive Portal redirect name is set to “captive-portal.com”.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to revert the URL name back to the default “captive-portal.com”.

- Use this command to change the Captive Portal redirect URL name to match the common name (cn) used by the public certificate on the switch. Matching these two names prevents a certificate warning message caused when these names do not match.

**Note.** Do not preface the redirect URL domain name with `https://`; the switch automatically adds `https://` to the beginning of the domain name.

- When a device is classified into a UNP profile that has the Captive Portal authentication attribute enabled, the device is placed into a Captive Portal pre-login state. In this state, the device can contact a DHCP server to get an IP address and get the DNS server address.

- Initial HTTP requests received from a user device are responded to with the Captive Portal redirect name. The user device contacts the DNS server to resolve the redirect name and receives the Captive Portal IP address. Requests are then sent to the Captive Portal IP address that is mapped internally to the OmniSwitch web server, which then presents login Web pages to the user device.

- Make sure the DNS server configuration reflects the same Captive Portal name and IP address that is configured for the OmniSwitch.
Examples

-> captive-portal name cert-name
-> captive-portal name "20.2.2.1"
-> no captive-portal name

Release History

Release 8.1.1; command was introduced.

Related Commands

captive-portal ip-address
Configures the internal Captive Portal IP address for the switch.

show captive-portal configuration
Displays the global Captive Portal configuration for the switch.

MIB Objects

alaDaCPortalGlobalConfig
alaDaCPortalRedirectUrlName
captive-portal ip-address

Configures the internal Captive Portal IP address for the switch.

captive-portal ip-address ip_address

**Syntax Definitions**

*ip_address* IPv4 network address (e.g., 10.0.0.0, 171.15.0.0, 196.190.254.0).

**Defaults**

By default, the internal Captive Portal IP address is set to 10.123.0.1.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the default 10.123.0.0 subnet is already in use, then use this command to change the Captive Portal IP address to another 10.x.0.0 subnet (only the second octet of the Captive Portal IP address can be changed).

- When a device is classified into a UNP profile that has the Captive Portal authentication attribute enabled, the device is placed into a Captive Portal pre-login role. In this state, the device can contact a DHCP server to get an IP address and get the DNS server address.

- Initial HTTP requests received from a user device are responded to with the Captive Portal redirect name. The user device contacts the DNS server to resolve the redirect URL name and receives the Captive Portal IP address. Requests are then sent to the Captive Portal IP address that is mapped internally to the OmniSwitch web server, which then presents login web pages to the user device.

- Make sure the DNS server configuration reflects the same Captive Portal name and IP address that is configured for the OmniSwitch.

**Examples**

```
-> captive-portal ip-address 10.255.0.20
```

**Release History**

Release 8.1.1; command was introduced.
**Related Commands**

- **captive-portal name**
  - Configures the name of the redirect URL that is used for accessing a public certificate.

- **show captive-portal configuration**
  - Displays the global Captive Portal configuration for the switch.

**MIB Objects**

- `alaDaCPortalGlobalConfig`
- `alaDaCPortalIpAddress`
captive-portal success-redirect-url

Configures the URL of a specific site to which a user is redirected after a successful Captive Portal authentication.

```
captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
```

**Syntax Definitions**

`redirect_url` The redirect URL (up to 63 characters).

**Defaults**

By default, no success redirect URL is configured.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to remove the success redirect URL from the Captive Portal global configuration.

**Examples**

```
-> no captive-portal success-redirect-url
```

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- `show captive-portal configuration` Displays the global Captive Portal configuration for the switch.

**MIB Objects**

- `alaDaCPortalGlobalConfig`
- `alaDaCPortalSuccRedirectUrl`
captive-portal proxy-server-port

Configures the proxy server port to use for Captive Portal.

captive-portal proxy-server-port proxy_port

no captive-portal proxy-server-port

Syntax Definitions

proxy_port The HTTP proxy port number. The valid range is 1024–49151.

Defaults

By default, the proxy server port number is set to 8080.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `no` form of this command to set the proxy port number back to the default (8080).
- This command overwrites the existing proxy port number for the switch.
- The proxy port number only requires changing if the proxy port used is not 80 or 8080.

Examples

- `-> captive-portal proxy-server-port 1200`
- `-> no captive-portal proxy-server-port`

Release History

Release 8.1.1; command was introduced.
Related Commands

show captive-portal configuration

Displays the global Captive Portal configuration for the switch.

MIB Objects

alaDaCPortalGlobalConfig
alaDaCPortalProxyPort
captive-portal retry-count

Configures the number of times a device can try to login before Captive Portal determines that authentication for that device has failed.

captive-portal retry-count retries

Syntax Definitions

retries The number of login attempts allowed. The valid range is 1–99.

Defaults

By default, the retry count is set to 3.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

No access page is sent to devices that exceed the number of login retries allowed.

Examples

-> captive-portal retry-count 5

Release History

Release 8.1.1; command was introduced.

Related Commands

show captive-portal configuration Displays the global Captive Portal configuration for the switch.

MIB Objects

alaDaCPortalGlobalConfig
alaDaCPortalRetryCnt
captive-portal authentication-pass

Configures a global authentication pass policy. This type of policy is applied to all devices successfully authenticated through the Captive Portal process. Each policy can specify a QoS policy list and UNP profile name to assign to the authenticated devices.

```
captive-portal authentication-pass {policy-list list_name | profile profile_name | profile-change {enable | disable}}
```

```
no captive-portal authentication-pass {policy-list | profile}
```

### Syntax Definitions

- **list_name**: The name of a QoS policy list to apply to the authenticated user device.
- **profile_name**: The name of an existing UNP profile.
- **enable**: Enables the profile change operation. Authenticated devices are assigned to the specified profile name.
- **disable**: Disables the profile change operation. Authenticated devices are not assigned to a new profile.

### Defaults

By default, no policy list name or UNP profile name is specified for the global Captive Portal configuration.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>9900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to remove the Captive Portal authentication pass policy from the global Captive Portal configuration.

- When the **profile-change** parameter is enabled, the profile initially assigned to the Captive Portal users is changed to the profile derived through successful Captive Portal authentication. The QoS policy list associated with the new profile is applied to the authenticated users.

- When a profile change occurs, the new profile may assign a different VLAN to the authenticated device. This new VLAN assignment is functional only after a port bounce or pause timer operation is completed. Existing Bring Your Own Device (BYOD) global commands are leveraged to configure the port bounce and pause timer values.

- If the new UNP profile assigned also has Captive Portal authentication enabled, the process is not started again. The results from the initial Captive Portal authentication process are used instead.
- When the `profile-change` parameter is disabled, the QoS policy list name returned from the RADIUS server or the list name specified with this command is applied instead.

- The QoS policy list to apply to Captive Portal authenticated devices is derived through one of the following methods:
  - The policy list name returned from the RADIUS server.
  - The policy list name specified with this command for the global Captive Portal configuration.
  - The policy list name associated with the UNP profile returned from the RADIUS server.
  - The policy list name associated with the UNP profile specified with this command for the global Captive Portal configuration.

- A policy list name or a UNP profile name returned from the RADIUS server takes precedence over the policy list name or UNP profile name configured through this command.

**Examples**

```
-> captive-portal authentication-pass policy-list list1
-> captive-portal authentication-pass profile unp1-vlan profile-change enable
-> captive-portal authentication-pass profile-change disable
-> no captive-portal authentication-pass policy-list
-> no captive-portal authentication-pass profile
```

**Release History**

Release 8.1.1; command was introduced.
Release 8.2.1; `edge-profile` and `edge-profile-change` parameters added.
Release 8.3.1; `edge-profile` and `edge-profile-change` parameters changed to `profile` and `profile-change`.

**Related Commands**

- **captive-portal authentication-pass domain**
  - Configures a domain specific authentication pass policy to determine the QoS policy list or UNP profile name to apply to authenticated devices. This type of policy overrides the global Captive Portal configuration.

- **show captive-portal configuration**
  - Displays the global Captive Portal configuration for the switch.

**MIB Objects**

- `alaDaCPortalGlobalConfig`
- `alaDaCPortalPolicyListName`
- `alaDaCPortalUNPProfile`
- `alaDaCPortalUNPProfileChange`
captive-portal authentication-pass domain

Configures a domain specific authentication pass policy. This type of policy is applied to all devices within the specified domain that were successfully authenticated through the Captive Portal process.

```
captive-portal authentication-pass realm {prefix | suffix} domain domain_name {policy-list list_name | profile profile_name | profile-change {enable | disable}}
```

```
no captive-portal authentication-pass [realm {prefix | suffix} domain domain_name]
```

**Syntax Definitions**

- **prefix**
  Specifies a prefix domain name (for example, domain_name/user).
- **suffix**
  Specifies a suffix domain name (for example, user@domain_name)
- **domain_name**
  The domain name for the user device.
- **list_name**
  The name of a QoS policy list to apply to the authenticated user device.
- **profile_name**
  The name of an existing UNP profile.
- **enable**
  Enables the profile change operation. Authenticated devices are assigned to the specified profile name.
- **disable**
  Disables the profile change operation. Authenticated devices are not assigned to a new profile.

**Defaults**

By default, no domain specific authentication pass policy is configured for the Captive Portal process.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove the domain specific authentication pass policy from the Captive Portal configuration.
- Use the **realm prefix domain** or **realm suffix domain** parameter to apply the authentication policy list or UNP profile based on the domain name of the Captive Portal authenticated user device.
- If the **profile-change** parameter is enabled, the profile initially assigned to the Captive Portal user is changed to the profile derived through successful Captive Portal authentication. The QoS policy list associated with the new profile is then applied to the authenticated users.
- When a profile change occurs, the new profile may assign a different VLAN to the authenticated device. This new VLAN assignment is functional only after a port bounce or pause timer operation is performed.
completed. Existing Bring Your Own Device (BYOD) global commands are leveraged to configure the port bounce and pause timer values.

- If the new profile assigned to the user also has Captive Portal authentication enabled, the process is not started again. The results from the initial Captive Portal authentication process are used instead.

- If the profile-change parameter is disabled, then the QoS policy list name returned from the RADIUS server or the list name specified through the global (non-domain specific) Captive Portal configuration is applied.

- The QoS policy list to apply to Captive Portal authenticated devices is derived through one of the following methods:
  - The policy list name returned from the RADIUS server.
  - The policy list name specified with this command or through the global Captive Portal configuration.
  - The policy list name associated with the UNP profile returned from the RADIUS server.
  - The policy list name associated with the UNP profile specified with this command or through the global Captive Portal configuration.

- A policy list name or a UNP profile name returned from the RADIUS server takes precedence over the policy list name or UNP profile name configured through this command.

**Examples**

```
-> captive-portal authentication-pass realm prefix domain asia-pacific policy-list list2
-> captive-portal authentication-pass realm suffix domain north-america profile unp2 profile-change enable
-> no captive-portal authentication-pass realm suffix domain north-america
```

**Release History**

Release 8.1.1; command was introduced.
Release 8.2.1; edge-profile and edge-profile-change parameters added.
Release 8.3.1; edge-profile and edge-profile-change parameters changed to profile and profile-change.

**Related Commands**

- **captive-portal authentication-pass**
  Configures a global authentication pass policy. This type of policy is applied to all devices successfully authenticated through the Captive Portal process.

- **show captive-portal configuration**
  Displays the global Captive Portal configuration for the switch.

**MIB Objects**

alaDaCPortalAuthPassTable
  - alaDaCPortalAuthDomainName
  - alaDaCPortalAuthRealm
  - alaDaCPortalAuthPolicyListName
  - alaDaCPortalAuthRowStatus
  - alaDaCPortalAuthUNPProfile
alaDaCPortalAuthUNPProfileChange
captive-portal-profile

Configures a Captive Portal profile that is assigned to a UNP profile. This type of profile defines Captive Portal configuration options that are applied to devices classified into the assigned UNP profile. This command page describes the base command (`captive-portal-profile profile_name`) along with the other command keywords that are used to configure profile attributes.

```plaintext
captive-portal-profile profile_name
   [aaa-profile aaa_profile_name]
   [success-redirect-url redirect_url]
   [retry-count retries]
   [authentication-pass [realm {prefix | suffix} domain domain_name] {policy-list list_name | profile profile_name | profile-change {enable | disable}}]

no captive-portal-profile profile_name
```

**Syntax Definitions**

- **profile_name**: The name to assign to the Captive Portal profile (up to 32 characters).
- **aaa_profile_name**: The name of an authentication, authorization, and accounting (AAA) profile to associate with the Captive Portal profile.
- **redirect_url**: A URL (up to 63 characters) to which user devices are redirected after successful Captive Portal authentication.
- **retries**: The number of login attempts allowed. The range is 1–99.
- **realm prefix**: Specifies a prefix domain name (for example, `domain_name/user`).
- **realm suffix**: Specifies a suffix domain name (for example, `user@domain_name`).
- **domain_name**: The domain name for the user device.
- **list_name**: The name of a QoS policy list to apply to the authenticated user device.
- **profile_name**: The name of an existing UNP profile.
- **enable**: Enables the profile change operation. Authenticated devices are assigned to the specified profile name.
- **disable**: Disables the profile change operation. Authenticated devices are not assigned to a new profile.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa_profile_name</td>
<td>none</td>
</tr>
<tr>
<td>redirect_url</td>
<td>none</td>
</tr>
<tr>
<td>retries</td>
<td>3</td>
</tr>
<tr>
<td>realm prefix</td>
<td>suffix</td>
</tr>
<tr>
<td>domain_name</td>
<td>none</td>
</tr>
<tr>
<td>list_name</td>
<td>none</td>
</tr>
<tr>
<td>profile_name</td>
<td>none</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to remove the Captive Portal profile from the switch configuration.

- Creating a Captive Portal profile name with the base command (**captive-portal-profile profile_name**) is not required to configure a profile attribute value. If the profile name does not exist, the switch will automatically create the name specified when the attribute is configured. For example, the **unp captive-portal-profile cp-prof1 retry-count 5** command will create the “cp-prof1” profile if it does not already exist in the switch configuration.

- When a Captive Portal profile is applied to a UNP profile, the parameter values defined in the profile override the global Captive Portal parameter values configured for the switch.

- A Captive Portal profile is applied only when Captive Portal authentication is enabled for the UNP profile. If there is no Captive Portal profile associated with a UNP profile, then the global Captive Portal configuration is applied.

- Assigning an AAA profile to a Captive Portal profile defines specific AAA configuration options (such as RADIUS servers and RADIUS client attributes) that are used for Captive Portal authentication. If there is no AAA profile assigned, then the global AAA configuration is used.

- AAA profiles are configured using the **aaa profile** command. See the “AAA Commands” chapter in the **OmniSwitch AOS Release 8 CLI Reference Guide** for more information.

Examples

```
-> captive-portal-profile cp-p1
-> captive-portal-profile cp-p1 aaa-profile aaa_p1
-> captive-portal-profile cp-p1 authentication-pass realm prefix domain asia-pacific policy-list list1
-> no captive-portal-profile cp-p1 aaa-profile aaa_p1
-> no captive-portal-profile cp-p1

-> captive-portal-profile cp-p2 retry-count 5
-> captive-portal-profile cp-p2 authentication-pass profile ep-1
-> captive-portal-profile cp-p2 authentication-pass profile-change enable
-> captive-portal-profile cp-p2 authentication-pass profile-change disable
-> no captive-portal-profile cp-p2 authentication-pass profile
-> no captive-portal-profile cp-p2
```

Release History

Release 8.1.1; command was introduced.
Release 8.2.1; **edge-profile** and **edge-profile-change** parameters added.
Release 8.3.1; **edge-profile** and **edge-profile-change** parameters changed to **profile** and **profile-change**.
Related Commands

unp profile captive-portal-profile  Assigns a Captive Portal profile to a UNP profile.

aaa profile  Configures an AAA configuration profile.

show captive-portal profile-names  Displays the Captive Portal profile configuration for the switch.

MIB Objects

alaDaCPortalProfTable
  alaDaCPortalProfName
  alaDaCPortalProfSuccRedirectUrl
  alaDaCPortalProfRetryCnt
  alaDaCPortalProfAuthPolicyListName
  alaDaCPortalProfAaaProf
  alaDaCPortalProfUNPProfile
  alaDaCPortalProfUNPProfileChange

alaDaCPortalProfDomainTable
  alaDaCPortalProfDomainAuthDomainName
  alaDaCPortalProfDomainAuthPolicyListName
  alaDaCPortalProfDomainAuthRealm
  alaDaCPortalProfDomainUNPProfile
  alaDaCPortalProfDomainUNPProfileChange
captive-portal customization

Enables or disables the use of custom Web pages for Captive Portal authentication. When customization is enabled, Captive Portal presents Web pages stored in the “/flash/switch/captive_portal/custom_files/” directory on the switch. When customization is disabled, Captive Portal presents Web pages stored in the “/flash/switch/captive_portal/release_files/” directory on the switch.

captive-portal customization {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Displays custom web pages for Captive Portal authentication.</td>
</tr>
<tr>
<td>disable</td>
<td>Displays default web pages for Captive Portal authentication.</td>
</tr>
</tbody>
</table>

Defaults

By default, the web pages provided on the switch are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• To create custom Web pages, create a folder in the same path as the “release_files” folder and name the new folder “custom_files” (for example “/flash/switch/captive_portal/custom_files/”). Next, copy the “assets” and “templates” folders found under “/flash/switch/captive_portal/release_files/” to the “custom_files” folder. Modify the contents in the copied folders to create custom Web pages.

• The “release_files” folder is overwritten each time the switch reboots, so **DO NOT** modify the files in this folder for custom use.

• The folders "assets" and "templates" under the /flash/switch/captive_portal/custom_files/ directory are used to create and display Web pages to Captive Portal users when the switch reboots or at runtime when Captive Portal customization is enabled for the switch, if the “custom_files” folder exists.

• Anything in the custom "assets" folder is statically served by the internal Web server on the switch whenever they are requested. These pages are typically .css files, javascript files, or the acceptable use policy and are linked to files in the custom "templates" folder.

• The custom "templates" folder contains the Web pages that are dynamically served to users depending on the Captive Portal state of each user. The file names in this folder must not be changed. The login form field names and form action in these pages must not be changed. The variables in these pages, as denoted by "<?=$'(name)?>”, are substituted in place by the internal Web server.
Examples

- captive-portal customization enable
- captive-portal customization disable

Release History
Release 8.1.1; command was introduced.

Related Commands

show captive-portal configuration
Displays the global Captive Portal configuration for the switch.

MIB Objects

alaDaCPortalGlobalConfig
alaDaCPortalCustomization
show captive-portal configuration

Displays the global Captive Portal parameter settings configured for the switch.

show captive-portal configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Currently only the internal Captive Portal mode (Web server on the switch) is configurable for the switch. An external Captive Portal operation is provided through interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch BYOD solution.
- The parameter values configured and applied through a Captive Portal profile override any values set through the global Captive Portal configuration. A Captive Portal profile is associated with a UNP profile and is applied to devices classified into that profile.

Examples

-> show captive-portal configuration
Captive Portal Global Configuration:

- Captive Portal Mode = Internal
- DHCP Parameters:
  - DHCP Lease Time = 30
  - DHCP Renew Time = 15
  - DHCP Rebinding Time = 26
- Captive Portal IP address = 10.123.0.1
- Captive Portal Redirect String = captive-portal.com
- Captive Portal Success Redirect URL =
- Captive Portal Proxy Server Port = 8080
- Captive Portal Retry Count = 3
- Captive Portal Global Auth Policy List =
- Captive Portal Page Customization = Disable
- Captive Portal Profile Name =
Captive Portal Profile Change = Disable

Domain Specific Policy Lists:

<table>
<thead>
<tr>
<th>Domain</th>
<th>Realm</th>
<th>Policy List</th>
<th>Profile Name</th>
<th>Profile Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>na01</td>
<td>Suffix</td>
<td>qos-bw1</td>
<td>unp1-vlan</td>
<td>Enable</td>
</tr>
<tr>
<td>na02</td>
<td>Prefix</td>
<td>qos-bw2</td>
<td>unp2-vlan</td>
<td>Enable</td>
</tr>
</tbody>
</table>

### output definitions

- **Captive Portal Mode**
  The Captive Portal mode of operation. Only the internal and internal DHCP modes (Web server on the OmniSwitch) are supported at this time. Configured through the `captive-portal mode` command.

- **DHCP Parameters**:
  A list of DHCP parameter values that are applied when the internal DHCP mode is active. These fields display “N/A” when the internal DHCP mode is not active. Configured through the `captive-portal mode` command.

  - **DHCP Lease Time**
    The amount of time an IP address is leased to a DHCP client.

  - **DHCP Renew Time**
    The amount of time, in seconds, until an attempt is made to renew the leased IP address (50% of the DHCP Lease Time).

  - **DHCP Rebinding Time**
    The amount of time until an attempt is made to obtain a new IP leased address (87.5% of the DHCP Lease Time).

- **Captive Portal IP address**
  The internal Captive Portal IP address for the switch. Configured through the `captive-portal ip-address` command.

- **Captive Portal Redirect String**
  The name of the redirect URL that is used for accessing a public certificate. Configured through the `captive-portal name` command.

- **Captive Portal Success Redirect URL**
  The URL of a specific site to which a user is redirected after a successful Captive Portal authentication. Configured through the `captive-portal success-redirect-url` command.

- **Captive Portal Proxy Server Port**
  The proxy server port to use for Captive Portal. Configured through the `captive-portal proxy-server-port` command.

- **Captive Portal Retry Count**
  The number of times a device can try to login before Captive Portal determines that authentication for that device has failed. Configured through the `captive-portal retry-count` command.

- **Captive Portal Global Auth Policy List**
  The name of a QoS policy list for the global Captive Portal configuration. The specified list is applied to each device that passes Captive Portal authentication. Configured through the `captive-portal authentication-pass` command.

- **Captive Portal Page Customization**
  Whether or not (Enable or Disable) customized Captive Portal pages are presented to the user.

- **Captive Portal Profile Name**
  The name of a UNP profile for the global Captive Portal configuration. The specified profile is only applied to Captive Portal authenticated devices when the Captive Portal profile change option is enabled. Configured through the `captive-portal authentication-pass` command.

- **Captive Portal Profile Change**
  The status of profile change (Enable or Disable). When enabled, the profile initially assigned to the Captive Portal user is changed to the profile specified through the Captive Portal profile name option. Configured through the `captive-portal authentication-pass` command.
### output definitions

<table>
<thead>
<tr>
<th>Domain Specific Policy Lists:</th>
<th>A list of Captive Portal domain specific policies. The policy list is applied when the domain for a Captive Portal authenticated device matches the domain criteria associated with the list. Domain specific policies take precedence over the global Captive Portal settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>The domain name associated with a domain specific policy. Configured through the <code>captive-portal authentication-pass domain</code> command.</td>
</tr>
<tr>
<td>Realm</td>
<td>The realm of the domain name (<strong>prefix</strong> or <strong>suffix</strong>) associated with a domain specific policy. The realm identifies the domain name as a prefix (<code>domain-name/user</code>) or as a suffix (<code>user@domain-name</code>). Configured through the <code>captive-portal authentication-pass domain</code> command.</td>
</tr>
<tr>
<td>Policy List</td>
<td>The name of the QoS policy list that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the list name. Configured through the <code>captive-portal authentication-pass domain</code> command.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>The name of the UNP profile that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the profile name. Configured through the <code>captive-portal authentication-pass domain</code> command.</td>
</tr>
<tr>
<td>Profile Change</td>
<td>The status of profile change (<strong>Enable</strong> or <strong>Disable</strong>) for the associated domain name. When enabled, the initial profile assigned to the Captive Portal device is changed to the profile specified through the profile change option associated with the domain name. Configured through the <code>captive-portal authentication-pass domain</code> command.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.1.1; command was introduced.
Release 8.5R4; DHCP Parameter fields added.

### Related Commands

- **show captive-portal profile-names**
  - Displays the Captive Portal profile configuration for the switch.
MIB Objects

alaDaCPortalGlobalConfig
alaDaCPortalMode
alaDaCPortalDHCPLeaseTime
alaDaCPortalDHCPRenewTime
alaDaCPortalDHCPRebindingTime
alaDaCPortalIpAddress
alaDaCPortalRedirectUrlName
alaDaCPortalSuccRedirectUrl
alaDaCPortalProxyPort
alaDaCPortalRetryCnt
alaDaCPortalPolicyListName
alaDaCPortalCustomization
alaDaCPortalUNPProfile
alaDaCPortalUNPProfileChange
alaDaCPortalAuthPassTable
alaDaCPortalAuthDomainName
alaDaCPortalAuthRealm
alaDaCPortalAuthPolicyListName
alaDaCPortalAuthRowStatus
alaDaCPortalAuthUNPProfile
alaDaCPortalAuthUNPProfileChange
show captive-portal profile-names

Displays the Captive Portal profile configuration for the switch. The parameter values configured and applied through a Captive Portal profile override any values set through the global Captive Portal configuration.

show captive-portal {profile-names | profile-name profile_name configuration}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile-names</td>
<td>Displays a list of configured Captive Portal profiles.</td>
</tr>
<tr>
<td>profile-name</td>
<td>Displays the Captive Portal parameter configuration for the specified</td>
</tr>
<tr>
<td>configuration</td>
<td>profile name.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Currently only the internal Captive Portal mode (Web server on the switch) is configurable for the switch. An external Captive Portal operation is provided through interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch BYOD solution.

Examples

-> show captive-portal profile-names

  Captive Portal Profile Names
  -----------------------------
  1. cp1
  2. cp2
  3. cp3

-> show captive-portal profile-name cp1 configuration

Captive Portal Profile cp1 Configuration:
  Captive Portal Mode = Internal
  Captive Portal AAA Profile Name =
  Captive Portal Success Redirect URL =
  Captive Portal Retry Count = 3
  Captive Portal Global Auth Policy List =
Captive Portal Mode

The Captive Portal mode of operation. Only internal mode (Web server on the OmniSwitch) is supported at this time.

Captive Portal AAA Profile Name

The name of an authentication, authorization, and accounting (AAA) profile associated with the Captive Portal profile.

Captive Portal Success Redirect URL

The URL of a specific site to which a user is redirected after a successful Captive Portal authentication.

Captive Portal Retry Count

The number of times a device can try to login before Captive Portal determines that authentication for that device has failed.

Captive Portal Global Auth Policy List

The name of a QoS policy list for the global Captive Portal configuration. The specified list is applied to each device that passes Captive Portal authentication.

Captive Portal Profile Name

The name of a UNP profile for the global Captive Portal configuration. The specified profile is only applied to Captive Portal authenticated devices when the Captive Portal profile change option is enabled.

Captive Portal Profile Change

The status of profile change (Enable or Disable). When enabled, the profile initially assigned to the Captive Portal user is changed to the profile specified through the Captive Portal profile name option.

Domain Specific Policy Lists:

A list of Captive Portal domain specific policies. The policy list is applied when the domain for a Captive Portal authenticated device matches the domain criteria associated with the list. Domain specific policies take precedence over the global Captive Portal settings.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Realm</th>
<th>Policy List</th>
<th>Profile Name</th>
<th>Profile Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>na01</td>
<td>Suffix</td>
<td>qos-bw1</td>
<td>unp1-vlan</td>
<td>Enable</td>
</tr>
<tr>
<td>na02</td>
<td>Prefix</td>
<td>qos-bw2</td>
<td>unp2-vlan</td>
<td>Enable</td>
</tr>
</tbody>
</table>

output definitions

Captive Portal Mode

The Captive Portal mode of operation. Only internal mode (Web server on the OmniSwitch) is supported at this time.

Captive Portal AAA Profile Name

The name of an authentication, authorization, and accounting (AAA) profile associated with the Captive Portal profile.

Captive Portal Success Redirect URL

The URL of a specific site to which a user is redirected after a successful Captive Portal authentication.

Captive Portal Retry Count

The number of times a device can try to login before Captive Portal determines that authentication for that device has failed.

Captive Portal Global Auth Policy List

The name of a QoS policy list for the global Captive Portal configuration. The specified list is applied to each device that passes Captive Portal authentication.

Captive Portal Profile Name

The name of a UNP profile for the global Captive Portal configuration. The specified profile is only applied to Captive Portal authenticated devices when the Captive Portal profile change option is enabled.

Captive Portal Profile Change

The status of profile change (Enable or Disable). When enabled, the profile initially assigned to the Captive Portal user is changed to the profile specified through the Captive Portal profile name option.

Domain Specific Policy Lists:

A list of Captive Portal domain specific policies. The policy list is applied when the domain for a Captive Portal authenticated device matches the domain criteria associated with the list. Domain specific policies take precedence over the global Captive Portal settings.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Realm</th>
<th>Policy List</th>
<th>Profile Name</th>
<th>Profile Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>na01</td>
<td>Suffix</td>
<td>qos-bw1</td>
<td>unp1-vlan</td>
<td>Enable</td>
</tr>
<tr>
<td>na02</td>
<td>Prefix</td>
<td>qos-bw2</td>
<td>unp2-vlan</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Domain

The domain name associated with a domain specific policy.

Realm

The realm of the domain name (prefix or suffix) associated with a domain specific policy. The realm identifies the domain name as a prefix (domain-name/user) or as a suffix (user@domain-name).

Policy List

The name of the QoS policy list that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the list name.

Profile Name

The name of the UNP profile that is applied when the domain of a Captive Portal authenticated user device matches the domain criteria associated with the profile name.

Profile Change

The status of profile change (Enable or Disable) for the associated domain name. When enabled, the initial profile assigned to the Captive Portal device is changed to the profile specified through the profile change option associated with the domain name.
Release History

Release 8.1.1; command was introduced.

Related Commands

captive-portal-profile

Configures a Captive Portal profile.

show captive-portal configuration

Displays the global Captive Portal parameter settings configured for the switch

MIB Objects

alaDaCPortalProfTable
alaDaCPortalProfName
alaDaCPortalProfSuccRedirectUrl
alaDaCPortalProfRetryCnt
alaDaCPortalProfAuthPolicyListName
alaDaCPortalProfAaaProf
alaDaCPortalProfUNPProfile
alaDaCPortalProfUNPProfileChange
qmr quarantine path

Specifies the URL for a remediation server. This information is used by the Quarantine Manager and Remediation (QMR) application. A quarantined user is redirected to a remediation server to correct the condition that put the user into a quarantined state.

qmr quarantine path url

no qmr quarantine path

Syntax Definitions

url

The URL for the QMR remediation server.

Defaults

By default, no URL is configured.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of the command to remove the remediation server URL from the configuration.
- Make sure to add the corresponding IP address for the remediation server to the QMR list of exception subnets, configured through the qmr quarantine allowed-name command.
- Configuring the URL and adding the server IP address to the allowed list is required to redirect quarantined MAC addresses to the remediation server.
- Redirecting quarantined users learned on UNP access ports for remediation is not supported; users learned on UNP bridge ports can be redirected for remediation.

Examples

-> qos quarantine path www.remediate.com
-> no quarantine path

Release History

Release 8.1.1; command was introduced.
### Related Commands

- **qmr quarantine page**
  Configures whether or not QMR will send a “Quarantined” page to a user when a remediation server is not configured.

- **qmr quarantine allowed-name**
  Configures a list of IP addresses to which a restricted quarantined user can access.

- **qmr quarantine custom-proxy-port**
  Configures the HTTP proxy port number that is used to redirect traffic from a quarantined device.

- **qos quarantine mac-group**
  Configures the name of the Quarantine MAC address group.

- **show qmr**
  Displays the Access Guardian QMR configuration.

- **show quarantine mac group**
  Displays the contents of the QoS quarantined MAC address group.

### MIB Objects

- **alaDaQMRGlobalConfig**
- **alaDaQMRPath**
qmr quarantine page

Configures the QMR application to send a “Quarantined” page to a client if a remediation server is not configured. This page is used to notify the client that QMR has quarantined the client.

qmr qos quarantine page {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the sending of a “Quarantined” page to the client.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the sending of a “Quarantined” page to the client.</td>
</tr>
</tbody>
</table>

Defaults

By default, no “Quarantined” page is sent to the client.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

A “Quarantined” page is only sent if a remediation server path was not configured for QMR. Note that even if the remediation server is not active, QMR will not send the page as long as there is a value set for the remediation server path.

Examples

- `qmr quarantine page enable`
- `qmr quarantine page disable`

Release History

Release 8.1.1; command was introduced.
Related Commands

qmr quarantine path
  Specifies the URL for a remediation server.
qmr quarantine allowed-name
  Configures a list of IP addresses to which a restricted quarantined user can access.
qmr quarantine custom-proxy-port
  Configures the HTTP proxy port number that is used to redirect traffic from a quarantined device.
qos quarantine mac-group
  Configures the name of the Quarantine MAC address group.
show qmr
  Displays the Access Guardian QMR configuration.
show quarantine mac group
  Displays the contents of the QoS quarantined MAC address group.

MIB Objects

alaDaQMRGlobalConfig
  alaDaQMRPage
qmr quarantine allowed-name

Configures a list of IP addresses that a restricted quarantined user is allowed to access.

```
qmr quarantine allowed-name name ip-address ip_address [ip-mask ip_mask]
no qmr quarantine allowed-name name
```

**Syntax Definitions**

- **name**: Specify a name to assign to the allowed IP network address.
- **ip_address**: An IPv4 network address (for example, 10.0.0.0, 171.15.0.0, or 196.190.254.0).
- **ip_mask**: A valid IP address mask for the allowed IP network address (for example, 255.0.0.0 or 255.255.0.0)

**Defaults**

By default, no IP addresses are configured as QMR allowed addresses.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_mask</td>
<td>IP address class</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove an IP address from the allowed list.
- A maximum of two allowed IP addresses is supported.
- Make sure the IP address of the QMR remediation server is configured as an allowed IP address. A quarantined user is redirected to a remediation server to correct the condition that put the user into a quarantined state.

**Examples**

```
-> qmr quarantine allowed-name server2 ip-address 10.0.0.20 ip-mask 255.0.0.0
-> no qmr quarantine allowed-name server2
```
**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

- **qmr quarantine path**
  Specifies the URL for a remediation server.

- **qmr quarantine page**
  Configures whether or not QMR will send a “Quarantined” page to a user when a remediation server is not configured.

- **qmr quarantine custom-proxy-port**
  Configures the HTTP proxy port number that is used to redirect traffic from a quarantined device.

- **qos quarantine mac-group**
  Configures the name of the Quarantine MAC address group.

- **show qmr**
  Displays the Access Guardian QMR configuration.

- **show quarantine mac group**
  Displays the contents of the QoS quarantined MAC address group.

**MIB Objects**

- alaDaQMRAllowedTable
- alaDaQMRAllowedName
- alaDaQMRAllowedIpAddr
- alaDaQMRAllowedIpMask
**qmr quarantine custom-proxy-port**

Configures the HTTP proxy port number used in the Web browser configuration of a host device. Quarantine Manager uses this information when trapping HTTP packets from a quarantined device and redirecting traffic from the device for remediation.

```
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
```

**Syntax Definitions**

*proxy_port* 
The HTTP proxy port number. The valid range is 1025–65535.

**Defaults**

By default, the redirect proxy port number is set to 8080.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `no` form of this command to set the proxy port number back to 8080 (the default).

**Examples**

- `-> qmr quarantined custom-proxy-port 8887`
- `-> no qmr quarantined custom-proxy-port`

**Release History**

Release 8.1.1; command was introduced.
**Related Commands**

- `qmr quarantine path` Specifies the URL for a remediation server.
- `qmr quarantine page` Configures whether or not QMR will send a “Quarantined” page to a user when a remediation server is not configured.
- `qmr quarantine allowed-name` Configures a list of IP addresses to which a restricted quarantined user can access.
- `qos quarantine mac-group` Configures the name of the Quarantine MAC address group.
- `show qmr` Displays the Access Guardian QMR configuration.
- `show quarantine mac group` Displays the contents of the QoS quarantined MAC address group.

**MIB Objects**

- `alaDaQMRGlobalConfig`
- `alaDaQMRCustomHttpProxyPort`
show qmr

Displays the Quarantine Manager and Remediation (QMR) configuration for the switch.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>66465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

QMR is an OmniSwitch application that interacts with the OmniVista Quarantine Manager (OVQM) application to restrict the network access of quarantined clients and provide a remediation path for such clients to regain their network access. This command displays the OmniSwitch QMR configuration.

Examples

-> show qmr

Quarantine Mac Group Name : Quarantine,
Allowed IP Subnets : IT-HD 135.254.1.10 /255.255.255.248,
                     oss-lan 10.1.1.0 /255.255.255.0,
                     rem-ser 135.254.200.0 /255.255.255.0,
Custom Proxy port : 8888,
Quarantine Path : www.remediation-server.alu.com,
Quarantine Page : enabled,

output definitions

<table>
<thead>
<tr>
<th>Quarantine MAC Group Name</th>
<th>Allowed IP Subnets</th>
</tr>
</thead>
<tbody>
<tr>
<td>The name of the QoS Quarantine MAC address group. Configured through the <code>qos quarantine mac-group</code> command.</td>
<td>A list of IP network addresses that devices can still access while in a quarantined state. Configured through the <code>qmr quarantine allowed-name</code> command.</td>
</tr>
</tbody>
</table>
output definitions

**Custom Proxy port**  The HTTP proxy port number used for redirection of HTTP traffic from quarantined devices. Configured through the `qmr quarantine custom-proxy-port` command.

**Quarantine Path**  The URL of a remediation server to which a device is redirected when the device is quarantined. Configured through the `qmr quarantine path` command.

**Quarantine Page**  Whether or not QMR sends a “Quarantined” page notification to a quarantined user when there is no remediation server configuration. Configured through the `qmr quarantine page` command.

---

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

*show quarantine mac group*  Displays the contents of the QoS Quarantine MAC address group.

**MIB Objects**

alaQoSConfigTable
- alaQoSConfigQuarantineMacGroupName

alaDaQMRAllowedTable
- alaDaQMRAllowedName
- alaDaQMRAllowedIpAddr
- alaDaQMRAllowedIpMask

alaDaQMRGlobalConfig
- alaDaQMRCustomHttpProxyPort
- alaDaQMRPath
- alaDaQMRPage
**show quarantine mac group**

Displays the contents of the QoS Quarantine MAC address group.

```
show quarantine mac group
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The QoS MAC address group contains the MAC addresses of clients that the OmniVista Quarantine Manager (OVQM) application has quarantined. This command displays the quarantined MAC addresses that belong to this group.

**Examples**

```
-> show quarantine mac group
Group Name : Quarantine,
Number of MACs quarantined : 6,
00:00:00:11:11:1b,
00:00:00:11:11:1a,
00:00:00:11:11:19,
00:00:00:11:11:18,
00:00:00:11:11:17,
00:00:00:11:11:16,
```

**Release History**

Release 8.1.1; command was introduced.

**Related Commands**

`qos quarantine mac-group` Configures the name of the QoS Quarantine MAC address group.

**MIB Objects**

N/A
zeroconf mdns admin-state

Enables or disables the Multicast DNS (mDNS) relay on the switch.

zeroconf mdns admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>enable</th>
<th>Enable the mDNS relay on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disable the mDNS relay on the switch.</td>
</tr>
</tbody>
</table>

Defaults

The mDNS relay feature is disabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Apple devices use mDNS (multicast DNS) as the underlying protocol for Bonjour exchanges.
- When mDNS relay is disabled on the switch, mDNS packets are handled in the same manner as conventional packets.

Example

-> zeroconf mdns admin-state enable
-> zeroconf mdns admin-state disable

Release History

Release 8.4.1 R02; command introduced.
Related Commands

**zeroconf ssdp admin-state**  Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.

**show zeroconf**  Displays the zero configuration for the switch.

MIB Objects

*alaZeroConfMdnsAdminStatus*
zeroconf ssdp admin-state

Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch. SSDP relay enables the OmniSwitch to allow non-Apple devices to discover services with minimal configuration by the administrator.

```
zeroconf ssdp admin-state {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the SSDP relay on the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the SSDP relay on the switch.</td>
</tr>
</tbody>
</table>

**Defaults**

The SSDP relay feature is disabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The Digital Living Network Alliance (DLNA) uses Universal Plug and Play (UPnP) for media management, discovery, and control. DLNA/UPnP uses SSDP to discover services, similar to how Bonjour uses mDNS for the same. All the SSDP packets coming in on an OmniSwitch are intercepted and tunneled through the GRE tunnel to the WLAN controller (acting as a gateway).

- When SSDP relay is disabled on the switch, SSDP packets are handled in the same manner as conventional packets.

**Example**

```
-> zeroconf ssdp admin-state enable
-> zeroconf ssdp admin-state disable
```

**Release History**

Release 8.4.1 R02; command introduced.
Access Guardian Commands

zeroconf ssdp admin-state

Related Commands

- `zeroconf mdns admin-state` Enables or disables the Multicast DNS (mDNS) relay on the switch.
- `show zeroconf` Displays the zero configuration for the switch.

MIB Objects

- `alaZeroConfSsdpAdminStatus`
zeroconf mode

Configures the mode of the SSDP or MDNS packet processing.

zeroconf mode [tunnel [type standard] | gateway | responder]

Syntax Definitions

tunnel This is Aruba mode. The packets are sent to the responder through the configured GRE tunnel with protocol value of 0x0. The tunnel mode is configured on the edge switch.

tunnel type standard The packets are sent to the responder through the configured GRE tunnel with protocol value of 0x6558.

gateway The received packets are forwarded to all the VLANs in the gateway VLAN list. The gateway mode is configured on the gateway switch.

responder This is responder mode. The responder mode is configured on the core switch. Responder mode is not supported on an OmniSwitch 6360 or OmniSwitch 9900.

Defaults

The tunnel mode (Aruba mode) is enabled by default.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- In tunnel mode (both Aruba and Standard), the responder IP address must be configured to tunnel the mDNS or SSDP packets. The operational status will be DOWN until the responder IP address is configured.

- In tunnel mode (both Aruba and Standard) or responder mode, the mDNS and SSDP packets are processed only when the Loopback0 IP address is configured, which is considered as the source IP address for the tunneled packets. Use the `ip interface` command to configure the interface address.

- In responder mode, the tunnel for each edge switch must be configured manually.

- In responder mode if there are no service rules configured, the responder switch will learn all the services but will not process any query received from the mDNS or SSDP client.

- The switch can operate in only one mode at a time.
**Example**

```
-> zeroconf mode gateway
-> zeroconf mode tunnel
-> zeroconf mode responder
```

**Release History**

Release 8.4.1 R02; command introduced.

**Related Commands**

- `zeroconf mdns admin-state` Enables or disables the Multicast DNS (mDNS) relay on the switch.
- `zeroconf ssdp admin-state` Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
- `zeroconf responder-ip` Configures the IP address of the tunnel endpoint (zero configuration responder).
- `zeroconf gateway-vlan-list` Adds or deletes a VLAN from the gateway VLAN list
- `zeroconf access-vlan-list` Adds or deletes a VLAN from the access VLAN list.
- `show zeroconf` Displays the zero configuration for the switch.

**MIB Objects**

```
alafZeroConfMode
    alafZeroConfTunnelMode
```
zeroconf responder-ip

Configures the IP address of the tunnel endpoint (zero configuration responder) on the edge switch.

zeroconf responder-ip ip_address

no zeroconf responder-ip ip_address

Syntax Definitions

ip_address The IPv4 address of the zero configuration responder.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>6900</th>
<th>X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Only IPv4 address can be configured as a responder IP address.
- In gateway mode, the responder IP address must not be configured.
- In tunnel mode, the responder IP address must be configured to tunnel the mDNS or SSDP packets. The operational status will be DOWN until the responder IP address is configured.
- To remove the responder IP address configuration, use the no form of the command.

Example

-> zeroconf responder-ip 10.0.0.1
-> no zeroconf responder-ip 10.0.0.1

Release History

Release 8.4.1 R02; command introduced.
**Related Commands**

- **zeroconf mdns admin-state**: Enables or disables the Multicast DNS (mDNS) relay on the switch.
- **zeroconf ssdp admin-state**: Enables or disables the Simple Service Discovery Protocol (SSDP) relay on the switch.
- **zeroconf mode**: Configures the mode of the SSDP or MDNS packet processing.
- **show zeroconf**: Displays the zero configuration for the switch.

**MIB Objects**

- `alaZeroConfResponderIpAddr`
- `alaZeroConfResponderIpAddressType`
zeroconf gateway-vlan-list

Adds or deletes a VLAN from the gateway VLAN list.

zeroconf gateway-vlan-list vlan_id1...vlan_idn

no zeroconf gateway-vlan-list vlan_id1...vlan_idn

Syntax Definitions

- **vlan_id**: The existing VLAN ID to be added or deleted from the gateway VLAN list. The valid range is 1-4094.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The gateway VLAN list can be configured only in the gateway mode.
- A maximum of 10 gateway VLANs is supported.
- To remove a VLAN from the gateway VLAN list, use the **no** form of the command.

Example

- `-> zeroconf gateway-vlan-list 1 2 4`
- `-> no zeroconf gateway-vlan-list 4`

Release History

Release 8.4.1 R02; command introduced.

Related Commands

- **zeroconf mode**: Configures the mode of the SSDP or mDNS packet processing.
- **show zeroconf**: Displays the zero configuration for the switch.
MIB Objects

alaZeroConfGatewayVlanTable
alaZeroConfGatewayVlanEntry
zeroconf access-vlan-list

Adds or deletes a VLAN from the access VLAN list.

```
zeroconf access-vlan-list vlan_id1...vlan_idn
no zeroconf access-vlan-list vlan_id1...vlan_idn
```

**Syntax Definitions**

- `vlan_id` The existing VLAN ID to be added or deleted from the access VLAN list. The valid range is 1-4094.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The access VLAN list must be configured when the tunnel mode use GRE tunnel type standard.
- The query packets from the responder is sent to the VLANs configured in the access VLAN list.
- A maximum of 16 access VLANs is supported.
- To remove a VLAN from the access VLAN list, use the `no` form of the command.

**Example**

```
-> zeroconf access-vlan-list 6 7 9
-> no zeroconf access-vlan-list 7
```

**Release History**

Release 8.4.1 R02; command introduced.
Related Commands

zeroconf mode
Configures the mode of the SSDP or mDNS packet processing.

show zeroconf
Displays the zero configuration for the switch.

MIB Objects

alaZeroConfAccessVlanTable
alaZeroConfAccessVlanEntry
zeroconf server-policy

Configures the server policy.

```
zeroconf server-policy policy_name [role | vlan | location | username | mac-address]
```

```
no zeroconf server-policy policy_name [role | vlan | location | username | mac-address]
```

### Syntax Definitions

- **policy_name**
  - The name of the zero configuration server policy. The policy name can be maximum 31 characters in length.

- **unp-name**
  - The name of a user-defined UNP role to map to the server policy. Multiple roles can be mapped to a server policy. The role name can be maximum 32 characters in length.

- **vlan**
  - The VLAN ID to be mapped with the server policy. Multiple VLAN IDs can be mapped to a server policy.

- **location**
  - The location name to be mapped with the server policy. Multiple locations can be mapped to a server policy. The location name can be maximum 63 characters in length.

- **username**
  - The user name to be mapped with the server policy. Multiple user names can be mapped to a server policy. The user name can be maximum 63 characters in length.

- **mac-address**
  - The MAC address to be mapped with the server policy. Multiple mac-address can be mapped to a server policy. Maximum size of mac-address allowed is six bytes.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The configured server policy is not applied unless it is mapped to a service rule.

- A maximum of 16 roles, 16 locations, 16 VLANs, 16 username, and 16 MAC address can be configured for a server policy.

- The server policy can be modified even when it is mapped to a service rule.
The server policy cannot be deleted if it is being used by a service rule.

The server policy attribute can be deleted even when it is mapped to a service rule unless any one of the policy attributes remains configured for that policy.

To remove the server policy, use the `no` form of the command. To remove specific attribute associated to the policy mention the attribute along with the `no` command.

**Example**

```plaintext
-> zeroconf server-policy SP1 role employee
-> zeroconf server-policy SP1 vlan 10 20 30
-> zeroconf server-policy SP1 location meetingroom1 meetingroom2
-> zeroconf server-policy SP1 username user1 user2
-> zeroconf server-policy SP1 mac-address e8:e7:32:9a:53:3 e8:e7:32:9a:53:3
-> no zeroconf server-policy SP1
-> no zeroconf server-policy SP1 role employee
-> no zeroconf server-policy SP1 vlan 10 20
-> no zeroconf server-policy SP1 location meetingroom1
-> no zeroconf server-policy SP1 username user2
-> no zeroconf server-policy SP1 mac-address e8:e7:32:9a:53:3
```

**Release History**

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; `username` and `mac-address` parameters included.
Release 8.7.R2; `role` parameter name changed to `unp-name`; `policy_name`, `username`, and `location` maximum numbers updated.

**Related Commands**

- `zeroconf mode` Configures the mode of the SSDP or mDNS packet processing.
- `zeroconf client-policy` Configures the client policy.
- `zeroconf service-rule policy` Defines service rules for selective sharing of services with the clients.
- `show zeroconf` Displays the zero configuration for the switch.
- `show zeroconf server policies` Displays the information of the server policies configured.

**MIB Objects**

- `alaZeroConfServerPolicyTable` Contains the server policy table.
- `alaZeroConfServerPolicyEntry` Represents a server policy entry.
- `alaZeroConfServerPolicyName` Policy name.
- `alaZeroConfServerRoleMappingName` Role mapping name.
- `alaZeroConfServerVlanMappingId` Vlan mapping id.
- `alaZeroConfServerLocationMappingString` Location mapping string.
- `alaZeroConfServerUsernameMappingString` Username mapping string.
- `alaZeroConfServerMacAddressMapping` Mac address mapping.
**zeroconf client-policy**

Configures the client policy.

```
zeroconf client-policy policy_name [role | vlan | location | username | mac-address]
```

```
no zeroconf client-policy policy_name [role | vlan | location | username | mac-address]
```

**Syntax Definitions**

- `policy_name`: The name of the zero configuration client policy. The policy name can be maximum 31 characters in length.
- `unp-name`: The name of a user-defined UNP role to map to the client policy. A maximum of 16 roles can be mapped to a client policy. The role name can be maximum 32 characters in length.
- `vlan`: The VLAN ID to be mapped with the client policy. Multiple VLAN IDs can be mapped to a client policy.
- `location`: The location name to be mapped with the client policy. Multiple locations can be mapped to a client policy. The location name can be maximum 63 characters in length.
- `username`: The user name to be mapped with the client policy. Multiple user names can be mapped to a client policy. The user name can be maximum 63 characters in length.
- `mac-address`: The MAC address to be mapped with the client policy. Multiple MAC addresses can be mapped to a client policy. Maximum size of MAC address allowed is 6 bytes.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The configured client policy is not applied unless it is mapped to a service rule.
- A maximum of 64 service rules can be configured.
- A maximum of 16 roles, 16 locations, 16 VLANs, 16 username, and 16 MAC address can be configured for a client policy.
The client policy can be modified even when it is mapped to a service rule.

The client policy cannot be deleted if it is being used by a service rule.

The client policy attribute can be deleted even when it is mapped to a service rule unless any one of the policy attributes remains configured for that policy.

To remove the client policy, use the no form of the command. To remove specific attribute associated to the policy mention the attribute along with the no command.

**Example**

```
- zeroconf client-policy SP1 role employee
- zeroconf client-policy SP1 vlan 10 20 30
- zeroconf client-policy SP1 location meetingroom1 meetingroom2
- zeroconf client-policy SP1 username username1 username2
- zeroconf client-policy SP1 mac-address e8:e7:32:9a:53:3 e8:e7:32:9a:53:3
- no zeroconf client-policy SP1
- no zeroconf client-policy SP1 role employee
- no zeroconf client-policy SP1 vlan 10 20
- no zeroconf client-policy SP1 location meetingroom1
- no zeroconf client-policy SP1 username user2
- no zeroconf client-policy SP1 mac-address e8:e7:32:9a:53:3
```

**Release History**

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **username** and **mac-address** parameters included.
Release 8.7R2; **role** parameter name changed to **unp-name**; **policy_name**, **username**, and **location** maximum numbers updated.

**Related Commands**

- **zeroconf mode** Configures the mode of the SSDP or mDNS packet processing.
- **zeroconf server-policy** Configures the server policy.
- **zeroconf service-rule policy** Allows to define service rules for selective sharing of services with the clients.
- **show zeroconf** Displays the zero configuration for the switch.
- **show zeroconf client policies** Displays the information of the client policies configured on the responder.

**MIB Objects**

- a1aZeroConfClientPolicyTable
  - a1aZeroConfClientPolicyEntry
  - a1aZeroConfClientPolicyName
  - a1aZeroConfClientRoleMappingName
  - a1aZeroConfClientVlanMappingId
  - a1aZeroConfClientLocationMappingString
  - a1aZeroConfClientUsernameMappingString
  - a1aZeroConfClientMacAddressMapping
**zeroconf service-rule policy**

Defines service rules for selective sharing of services with the clients.

`zeroconf service-rule rule_name server-policy server_policy_name client-policy client_policy_name`

`no zeroconf service-rule rule_name`

---

**Syntax Definitions**

- `rule_name` The name of the service rule. The rule name can be maximum 31 characters in length.
- `server_policy_name` Name of the server policy to be mapped with service rule. A server policy cannot be mapped to multiple service rules.
- `client_policy_name` The name of the client policy to be mapped with the service rule. A client policy cannot be mapped to multiple service rules.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- There must be one-to-one mapping between the server and client policy.
- The responder will respond to a service query only when the server and client policy is matched.
- A service rule with an existing server and client policy mapping cannot be linked to a new server and client policy without deleting the existing mapping.
- A maximum of 64 service rule configuration is supported on a responder.
- To remove a service rule, use the `no` form of the command.

---

**Example**

```
-> zeroconf service-rule SR1 server-policy SP1 client-policy CP1
-> no zeroconf service-rule SR1
```
**Release History**

Release 8.4.1 R02; command introduced.
Release 8.7R2; rule_name maximum number changed.

**Related Commands**

- **zeroconf mode** Configures the mode of the SSDP or mDNS packet processing.
- **zeroconf server-policy** Configures the server policy.
- **zeroconf client-policy** Configures the client policy.
- **zeroconf service-rule service-id** Configures selective services for a service rule to be shared with the clients.
- **show zeroconf** Displays the zero configuration for the switch.
- **show zeroconf service rules** Displays the information of the service rules configured on the responder.

**MIB Objects**

alaZeroConfServiceRuleTable
  - alaZeroConfServiceRuleEntry
  - alaZeroConfServiceRuleName
  - alaZeroConfServiceRuleServerPolicyName
  - alaZeroConfServiceRuleClientPolicyName
**zeroconf service-rule service-id**

Configures selective services for a service rule.

```
zeroconf service-rule rule_name [mdns-service-id | ssdp-service-id] service_id1....[service_idn]
no zeroconf service-rule rule_name [mdns-service-id | ssdp-service-id] service_id1....[service_idn]
```

**Syntax Definitions**

- **rule_name**
  The name of the service rule.

- **mdns-service-id**
  Configures the mDNS service ID list to be mapped with the service rule.

- **ssdp-service-id**
  Configures the SSDP service ID list to be mapped with the service rule.

- **service_id**
  The service ID to be mapped with the service rule. Multiple service IDs can be mapped with a service rule.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A service ID can be part of multiple service rule or multiple service IDs can be mapped to a service rule.

- A service ID can be mapped or removed from a service rule without deleting the service rule.

- The responder will respond to a service query only when the server and client policy is matched.

- A maximum of 64 service IDs can be configured for a service rule.

- To remove a service ID, use the **no** form of the command.

**Example**

```
-> zeroconf service-rule SR1 mdns-service-id _scanner._tcp.local _ipp._tcp.local
-> zeroconf service-rule SR2 ssdp-service-id urn:schemas-upnp-org:device:MediaServer:1 upnp:rootdevice
-> no zeroconf service-rule SR1 mdns-service-id _scanner._tcp.local
-> no zeroconf service-rule SR2 ssdp-service-id upnp:rootdevice
```
**Release History**

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; `ssdp-service-id` parameter added.

**Related Commands**

- `zeroconf service-rule policy` Defines service rules for selective sharing of services with the clients.
- `show zeroconf` Displays the zero configuration for the switch.
- `show zeroconf service rules` Displays the information of the service rules configured on the responder.

**MIB Objects**

alaZeroConfServiceRuleMdnsServiceMappingTable
alaZeroConfServiceRuleMdnsServiceMappingEntry
alaZeroConfServiceRuleSsdpServiceMappingEntry
**zeroconf service-list**

Configures a list of known services for mDNS or SSDP service query.

```
zeroconf [mdns service-list | ssdp service-list] service_id1...service_idn
no zeroconf [mdns service-list | ssdp service-list] service_id1...service_idn
```

### Syntax Definitions

- **mdns service-list**: Configures the list of mDNS services for the service query.
- **ssdp service-list**: Configure the list of SSDP services for the service query.
- **service_id**: The service ID to be included in the service list. A maximum of 64 service IDs can be configured in the list. The service ID can be maximum 63 characters in length.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The services in the list are queried for re-learning by the responder, in an event of reload or takeover on the responder.
- A maximum of 64 service IDs can be configured in a service list.
- To remove a service ID from the service list, use the `no` form of the command.

### Example

```
-> zeroconf mdns service-list _scanner._tcp.local _ipp._tcp.local
-> zeroconf ssdp service-list urn:schemas-upnp-org:device:MediaServer:1
upnp:rootdevice
-> no zeroconf mdns service-list _scanner._tcp.local
-> no zeroconf ssdp service-list upnp:rootdevice
```

### Release History

- Release 8.4.1 R02; command introduced.
- Release 8.4.1 R03; ssdp service-list parameter added.
- Release 8.7R2; service_id maximum number changed.
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>zeroconf service-id query-request</code></td>
<td>Queries a specific service.</td>
</tr>
<tr>
<td><code>show zeroconf services-cache</code></td>
<td>Displays the list of services assigned along with the service information.</td>
</tr>
<tr>
<td><code>show zeroconf</code></td>
<td>Displays the zero configuration for the switch.</td>
</tr>
</tbody>
</table>

## MIB Objects

- `alaZeroConfMdnsServiceTable`
- `alaZeroConfMdnsServiceEntry`
- `alaZeroConfSsdpServiceEntry`
zeroconf service-id query-request

Queries a specific service. If the responder does not learn a service, that specific service can be queried for re-learning by the responder.

```
zeroconf {mdns | ssdp} service-id service-id query-request
```

### Syntax Definitions

**mdns**

Sends mDNS query for the service ID to all the configured tunnels to re-learn the service instance.

**ssdp**

Sends SSDP query for the service ID to all the configured tunnels to re-learn the service instance.

**service_id**

The service ID to be queried for learning by the responder.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command to manually query for a specific service.

### Example

```
-> zeroconf mdns service-id _scanner._tcp.local query-request
-> zeroconf ssdp service-id upnp:rootdevice
```

### Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; ssdp parameter added.

### Related Commands

- **zeroconf mode**
  Configures the mode of the SSDP or mDNS packet processing.

- **show zeroconf**
  Displays the zero configuration for the switch.
**MIB Objects**

alaZeroConfMdnsServiceTriggerQuery
alaZeroConfSsdpServiceTriggerQuery
zeroconf edge-ip-list

Configures the list of tunnel edge endpoint IP addresses. The edge-ip-list must be configured for the responder.

**zeroconf edge-ip-list** ip_address1...ip_addressn

**no zeroconf edge-ip-list** ip_address1...ip_addressn

---

### Syntax Definitions

| ip_address | The tunnel edge endpoint IP address, which is the Loopback0 IP address of the edge switch. |

---

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The configured tunnel edge endpoint IP address in the list must be reachable. If the IP addresses are not reachable then the operational status of the mDNS will be down.

- To remove a tunnel edge endpoint IP address from the list, use the **no** form of the command.

### Example

- `-> zeroconf edge-ip-list 10.1.1.1 10.2.2.2 10.3.3.3`
- `-> no zeroconf edge-ip-list 10.1.1.1`

### Release History

Release 8.4.1 R02; command introduced.
**Related Commands**

- **zeroconf mode**  
  Configures the mode of the SSDP or mDNS packet processing.

- **show zeroconf edge-details**  
  Displays the IP address and reachability status of the tunnel endpoints configured on the responder.

- **show zeroconf**  
  Displays the zero configuration for the switch.

**MIB Objects**

- **alaZeroConfEdgeIpTable**
- **alaZeroConfEdgeIpEntry**
zeroconf edge-ip-list mode

Configures the edge IP mode as manual or auto.

zeroconf edge-ip-list mode [manual | auto]

Syntax Definitions

<table>
<thead>
<tr>
<th>manual</th>
<th>auto</th>
</tr>
</thead>
<tbody>
<tr>
<td>In this mode, the admin has to configure the edge IPs manually.</td>
<td>In this mode, edge IPs are automatically learned by the responder.</td>
</tr>
</tbody>
</table>

Defaults

By default, the mode is manual.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- By default, the mode is manual.
- In manual mode, the admin has to configure the edge IPs manually.

Example

- `-> zeroconf edge-ip-list mode manual`
- `-> zeroconf edge-ip-list mode auto`

Release History

Release 8.7 R1; command introduced.
Related Commands

zeroconf mode  Configures the mode of the SSDP or mDNS packet processing.
show zeroconf edge-details  Displays the IP address and reachability status of the tunnel endpoints configured on the responder.
show zeroconf  Displays the zero configuration for the switch.

MIB Objects

alaZeroConfEdgeIpTable
alaZeroConfEdgeIPMode
zeroconf refresh-database

Refreshes the database (mDNS or SSDP records) with latest server policies, client policies, server rules, learned service instances, and service cache entry.

*zeroconf {mdns | ssdp} refresh-database*

**Syntax Definitions**

**mdns**
- Refreshes the mDNS database. The files “mdns_srvr_pley”, “mdns_srvr_pley_inst”, “mdns_clnt_pley” and “mdns_srvc_rule” are updated.

**ssdp**
- Refreshes the SSDP database. The files “ssdp_srvr_pley”, “ssdp_srvr_pley_inst”, “ssdp_clnt_pley” and “ssdp_srvc_rule” are updated.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to update the latest server policies, server policy name along with learned service instance, client policies and server rules configuration.

- After refreshing the database, use the `show zeroconf services-cache` and `show zeroconf server policy-instances` commands to display the latest cache and service instances information.

**Example**

```
-> zeroconf mdns refresh-database
-> zeroconf ssdp refresh-database
```

**Release History**

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; `ssdp` parameter included.
**Related Commands**

- `show zeroconf services-cache` Displays the list of services learned by mDNS or SSDP stack.
- `show zeroconf server policy-instances` Displays the mDNS or SSDP service instance learned on the responder for each server policy.

**MIB Objects**

- `alaZeroConfMdnsActions`  
- `alaZeroConfSdnpActions`
show zeroconf

Displays the basic zero configuration details.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Example

-> show zeroconf
  zero-conf mode : responder,
  MDNS admin status : enabled,
  SSDP admin status : disabled
  MDNS operational status : up,
  SSDP operational status : down,
  Tunnel Source IP : 172.16.1.1

-> show zeroconf
  zero-conf mode : gateway,
  MDNS admin status : disabled,
  SSDP admin status : disabled
  MDNS operational status : down,
  SSDP operational status : down,
  Gateway vlans list : 1, 2, 3

-> show zeroconf
  zero-conf mode : tunnel,
  zero-conf tunnel type : standard,
  MDNS admin status : disabled,
  SSDP admin status : disabled
  MDNS operational status : down,
  SSDP operational status : down,
show zeroconf

-> show zeroconf

Responder IP            : -
Tunnel source IP        : -
Access vlans list       : 4, 5, 6
zero-conf mode          : tunnel,
zero-conf tunnel type   : aruba,
MDNS admin status       : disabled,
SSDP admin status       : disabled
MDNS operational status : down,
SSDP operational status : down,
Responder IP            : -
Tunnel source IP        : -

output definitions

<table>
<thead>
<tr>
<th>zero-conf mode</th>
<th>Displays the zero configuration mode configured.</th>
</tr>
</thead>
<tbody>
<tr>
<td>zero-conf tunnel type</td>
<td>Displays if the tunnel type is Aruba or Standard. This is displayed if the mode type is tunnel.</td>
</tr>
<tr>
<td>MDNS admin status</td>
<td>Displays the administrative status of the mDNS.</td>
</tr>
<tr>
<td>SSDP admin status</td>
<td>Displays the administrative status of the SSDP.</td>
</tr>
<tr>
<td>MDNS operational status</td>
<td>Displays the operational status of mDNS. The operation status will be down if the responder IP address is not configured or not reachable.</td>
</tr>
<tr>
<td>SSDP operational status</td>
<td>Displays the operational status of SSDP. The operation status will be down if the responder IP address is not configured or not reachable.</td>
</tr>
<tr>
<td>Responder IP</td>
<td>Displays the configured responder IP address. This is displayed if the mode type is tunnel.</td>
</tr>
<tr>
<td>Tunnel Source IP</td>
<td>Displays the source IP address of the tunnel. This is displayed if the mode type is tunnel or responder.</td>
</tr>
<tr>
<td>Gateway vlans list</td>
<td>Displays the configured gateway VLANs list. This is displayed if the mode type is gateway.</td>
</tr>
<tr>
<td>Access vlans list</td>
<td>Displays the configured access VLANs list. This is displayed if the mode type is tunnel and the tunnel type is standard.</td>
</tr>
</tbody>
</table>

Release History

Release 8.4.1 R02; command introduced.
Related Commands

- **zeroconf mdns admin-state**: Enables or disables mDNS tunnel relay for the switch.
- **zeroconf ssdp admin-state**: Associates a GRE tunnel interface with the mDNS relay feature.
- **zeroconf mode**: Configures the mode of the SSDP or MDNS packet processing.
- **zeroconf responder-ip**: Configures the IP address of the tunnel endpoint (zero configuration responder).
- **zeroconf gateway-vlan-list**: Adds or deletes a VLAN from the gateway VLAN list.
- **zeroconf access-vlan-list**: Adds or deletes a VLAN from the access VLAN list.

MIB Objects

alaZeroConfConfig
  - alaZeroConfMdnsAdminStatus
  - alaZeroConfSsdpAdminStatus
  - alaZeroConfMode
  - alaZeroConfTunnelMode
  - alaZeroConfResponderIpAddressType
  - alaZeroConfResponderIpAddress
  - alaZeroConfMdnsOperStatus
  - alaZeroConfSsdpOperStatus
**show zeroconf services**

Displays all the configured mDNS or SSDP service IDs.

```bash
show zeroconf [mdns | ssdp] services
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Learned</td>
<td>Learned</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Example

```bash
-> show zeroconf mdns services
Service Id                        CfgType
--------------------------------+-------------------
_ipp._tcp.local                   Configured
_printer._tcp.local               Learned

-> show zeroconf ssdp services
Service Id                        CfgType
--------------------------------+-------------------
upnp:rootdevice                   Configured
abcd:rootdevice                   Learned
```

### output definitions

<table>
<thead>
<tr>
<th>Service Id</th>
<th>Displays the name of the service ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CfgType</td>
<td>Displays if the service is a configured service or learned service.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; ssdp parameter added.
Related Commands

`zeroconf service-list`  Configures a list of known services for mDNS or SSDP service query.
`zeroconf service-rule policy`  Defines service rules for selective sharing of services with the clients.

MIB Objects

`alaZeroConfMdnsServiceTable`
  `alaZeroConfMdnsServiceEntry`
  `alaZeroConfMdnsServiceId`
  `alaZeroConfMdnsServiceType`
`alaZeroConfSsdpServiceTable`
  `alaZeroConfSsdpServiceEntry`
  `alaZeroConfSsdpServiceId`
  `alaZeroConfSsdpServiceType`
**show zeroconf services-cache**

Displays the list of services learned by mDNS or SSDP stack.

```
show zeroconf [mdns | ssdp] services-cache
```

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Example**

```
-> show zeroconf mdns services-cache
Service Instance: Officejet 7500 E910 [3EA581] (2)
Service-ID : _http-alt._tcp.local
IP address   : 18.6.1.7
Port         : 8080
Ttl          : 4500
Role         : Media_server
Location     : APPLE_printer_server_1111
User Name    : 88:51:fb:3e:a5:81
Mac          : 88:51:fb:3e:a5:81
Vlan         : 77

-> show zeroconf ssdp services-cache
Service Instance: uuid:00bc1f27-d258-4ad0-be79-d5e6ff4aee::upnp:rootdevice
Service-ID : urn:schemas-upnp-org:service:ConnectionManager:1
IP address   : 25.1.1.1
Port         : 42433
Ttl          : 1800
Role         : STUDENT_ACCESS
Location     : media_client_282137981273891723717387128937
User Name    : 00:0f:fe:26:9e:ad
Mac          : 00:0f:fe:26:9e:ad
Vlan         : 45
```
**Output definitions**

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Instance</td>
<td>Displays the device name of the service instance.</td>
</tr>
<tr>
<td>Service-ID</td>
<td>Displays the type of service.</td>
</tr>
<tr>
<td>IP address</td>
<td>Displays the IP address of the device on which the service is discovered.</td>
</tr>
<tr>
<td>Port</td>
<td>Displays the UDP port number of the discovered service instance.</td>
</tr>
<tr>
<td>TTL</td>
<td>Displays the age of the service cache entry in seconds.</td>
</tr>
<tr>
<td>Role</td>
<td>Displays the role derived from UNP policy list name on the edge switch.</td>
</tr>
<tr>
<td>Location</td>
<td>Displays the location derived from the edge switch.</td>
</tr>
<tr>
<td>User Name</td>
<td>Displays the user name assigned for the service.</td>
</tr>
<tr>
<td>Mac</td>
<td>Displays the MAC address assigned for the service.</td>
</tr>
<tr>
<td>Vlan</td>
<td>Displays the VLAN ID assigned for the service.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; **ssdp** parameter added.

**Related Commands**

- `zeroconf service-rule policy` Defines service rules for selective sharing of services with the clients.
- `zeroconf service-rule service-id` Configures selective services for a service rule to be shared with the clients.

**MIB Objects**

N/A
### show zeroconf edge-details

Displays the IP address and reachability status of the tunnel endpoints configured on the responder.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Example**

```
-> show zeroconf edge-details
EdgeIP mode : Manual
Edge count : 4
 EdgeIP     Status
-------------+---------
172.16.1.2   DOWN,
172.16.1.3   DOWN,
172.16.1.4   UP,
172.16.1.5   UP,
```

**output definitions**

- **EdgeIP**: The tunnel endpoint IP address configured on the responder.
- **Status**: The reachability status of the tunnel endpoint IP address.

**Release History**

- Release 8.4.1 R02; command introduced.
- Release 8.7 R1; “EdgeIP mode” and “Edge count” fields added to command output display
Related Commands

zeroconf edge-ip-list  Configures the list of tunnel edge endpoint IP addresses.

MIB Objects

alaZeroConfEdgeIpTable
  alaZeroConfEdgeIpEntry
  alaZeroConfEdgeIpAddrType
  alaZeroConfEdgeIpAddr
  alaZeroConfEdgeIpRowStatus
show zeroconf server policies

Displays information about the server policies configured.

show zeroconf server policies

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Example

-> show zeroconf server policies
Server policies:

Policy name : SP1
Attached locations : MMS_server_36_1_1_1
Attached roles : Media_server
Attached vlans : 55
Attached username : -
Attached mac : 00:0f:fe:3a:63:da

Policy name : printer1
Attached locations : -
Attached roles : -
Attached vlans : 1100
Attached username : -
Attached mac : -

output definitions

Policy name Displays the name of the server policy.
Attached roles Displays the role of the server policy.
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attached locations</td>
<td>Displays the location of the server policy.</td>
</tr>
<tr>
<td>Attached vlans</td>
<td>Displays the VLANs tagged to the server policy.</td>
</tr>
<tr>
<td>Attached username</td>
<td>Displays the username tagged to the server policy.</td>
</tr>
<tr>
<td>Attached mac</td>
<td>Displays the MAC address tagged to the server policy.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; “Attached username” and “Attached mac” output fields added.

**Related Commands**

**zeroconf server-policy**

Configures the server policy.

**MIB Objects**

alaZeroConfServerPolicyTable
alaZeroConfServerPolicyEntry
alaZeroConfServerPolicyName
alaZeroConfServerRoleMappingTable
alaZeroConfServerRoleMappingEntry
alaZeroConfServerRoleMappingName
alaZeroConfServerVlanMappingTable
alaZeroConfServerVlanMappingEntry
alaZeroConfServerVlanMappingId
alaZeroConfServerLocationMappingTable
alaZeroConfServerLocationMappingEntry
alaZeroConfServerLocationMappingString
show zeroconf client policies

Displays information about the client policies configured on the responder.

show zeroconf client policies

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Example**

-> show zeroconf client policies

Client policies:

```
Policy name         : CP1
Attached locations  : media_client_282137981273891723717387128937
Attached roles      : STUDENT_ACCESS
Attached vlans      : 45
Attached username   : -
Attached mac        : 00:0f:fe:3a:34:1a
```

**output definitions**

<table>
<thead>
<tr>
<th>Output Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy name</td>
<td>Displays the name of the client policy.</td>
</tr>
<tr>
<td>Attached roles</td>
<td>Displays the role of the client policy.</td>
</tr>
<tr>
<td>Attached locations</td>
<td>Displays the location of the client policy.</td>
</tr>
<tr>
<td>Attached vlans</td>
<td>Displays the VLANs tagged to the client policy.</td>
</tr>
<tr>
<td>Attached username</td>
<td>Displays the username tagged to the client policy.</td>
</tr>
<tr>
<td>Attached mac</td>
<td>Displays the MAC address tagged to the client policy.</td>
</tr>
</tbody>
</table>

---
**Release History**

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; “Attached username” and “Attached mac” output fields added.

**Related Commands**

zeroconf client-policy  Configures the client policy.

**MIB Objects**

alaZeroConfClientPolicyTable
alaZeroConfClientPolicyEntry
alaZeroConfClientPolicyName
alaZeroConfClientRoleMappingTable
alaZeroConfClientRoleMappingEntry
alaZeroConfClientRoleMappingName
alaZeroConfClientVlanMappingTable
alaZeroConfClientVlanMappingEntry
alaZeroConfClientVlanMappingId
alaZeroConfClientLocationMappingTable
alaZeroConfClientLocationMappingEntry
alaZeroConfClientLocationMappingString
alaZeroConfClientUsernameMappingTable
alaZeroConfClientUsernameMappingEntry
alaZeroConfClientUsernameMappingString
alaZeroConfClientMacAddressMappingTable
alaZeroConfClientMacAddressMappingEntry
alaZeroConfClientMacAddressMappingMacAddress
show zeroconf service rules

Displays information about the service rules configured on the responder.

show zeroconf service rules

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Example

-> show zeroconf service rules
Service rules:

Rule name : SR1
Client Policy : CP1
Server Policy : SP1
Attached mdns services : _ipp._tcp.local
Attached ssdp services : upnp:rootdevice

Rule name : SR2
Client Policy : CP2
Server Policy : SP2
Attached mdns services : _ipp._tcp.local
Attached ssdp services : upnp:rootdevice

Rule name : SR3
Client Policy : CP3
Server Policy : SP3
Attached mdns services : _ipp._tcp.local
Attached ssdp services : upnp:rootdevice
Output Definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule name</td>
<td>Displays the name of the service rule.</td>
</tr>
<tr>
<td>Client Policy</td>
<td>Displays the name of the client policy mapped to the service rule.</td>
</tr>
<tr>
<td>Server Policy</td>
<td>Displays the name of the server policy mapped to the service rule.</td>
</tr>
<tr>
<td>Attached mdns services</td>
<td>Displays the mDNS service instances learned for the service rule.</td>
</tr>
<tr>
<td>Attached ssdp services</td>
<td>Displays the SSDP service instances learned for the service rule.</td>
</tr>
</tbody>
</table>

Release History

Release 8.4.1 R02; command introduced.
Release 8.4.1 R03; “Attached ssdp services” output field added.

Related Commands

ceroconf service-rule policy  Defines service rules for selective sharing of services with the clients.

MIB Objects

alaZeroConfServiceRuleTable
  alaZeroConfServiceRuleEntry
  alaZeroConfServiceRuleName
  alaZeroConfServiceRuleServerPolicyName
  alaZeroConfServiceRuleClientPolicyName
**show zeroconf server policy-instances**

Displays the mDNS or SSDP service instance learned on the responder for each server policy.

```
show zeroconf [mdns | ssdp] server policy-instances
```

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Example**

```
-> show zeroconf mdns server policy-instances
MDNS server policy instances:

Policy name : SP1
Attached service instance : -

Policy name : SP2
Attached service instance : PRINTER_EDGE4
  PRINTER_EDGE3

Policy name : SP3
Attached service instance : -

Policy name : SP4
Attached service instance : PRINTER_EDGE4

-> show zeroconf ssdp server policy-instances
SSDP server policy instances:

Policy name : SP1
Attached service instance:

Policy name : SP3
```
Attached service instance: uuid:88618bb0-6790-4cb0-9166-e1d5af5a87c::upnp:rootdevice
Policy name: SP4
Attached service instance: uuid:88618bb0-6790-4cb0-9166-e1d5af5a87c::upnp:rootdevice

**output definitions**

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Displays the name of the server policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attached service instance</td>
<td>Displays the service instance learned for the server policy.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.4.1 R03; command introduced.

**Related Commands**

`zeroconf service-rule policy` Defines service rules for selective sharing of services with the clients.

**MIB Objects**

N/A
**show unp profile**

Displays the UNP profile configuration for the switch.

```
show unp profile [profile_name]
```

### Syntax Definitions

- **profile_name**
  - The name of the UNP to display.

### Defaults

By default, the configuration for all profiles is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a UNP profile name with this command to display information for a specific profile.
- Use the `show unp profile map` command to display the VLAN or service type (SPB, VXLAN, or static) that is mapped to the UNP profile.
- If Device Profiling is enabled for the switch, the following UNP profiles are automatically created on the switch and will be included in the display:
  - `devProfPrinter`
  - `devProfWindows`
  - `devProfIP-Phone`
  - `devProfWireless-Router`
  - `devProfSmartPhone/PDA/Tablets`

### Examples

```
-> show unp profile
Profile Name: unp2-spb
  Qos Policy = qrules1,
  Location Policy = -
  Period Policy = -
  CP Profile = -
  CP State = Dis
  Authen Flag = Dis
  Mobile Tag = Dis
  SAA Profile = -
```
show unp profile

Ingress BW = -, Egress BW = -, Ingress Depth = -, Egress Depth = -,
Inact Interval = 10, Mac-Mobility = Ena

Profile Name: unp1-vlan
Qos Policy = -, Location Policy = loclist1,
Period Policy = timelist1, CP Profile = guest-profile,
CP State = Dis, Authen Flag = Dis, Mobile Tag = Dis,
SAA Profile = -, Ingress BW = -, Egress BW = -, Ingress Depth = -, Egress Depth = -,
Inact Interval = 10, Mac-Mobility = Dis

Profile Name: defaultWLANProfile
Qos Policy = -, Location Policy = -, Period Policy = -, CP Profile = -,
CP State = Dis, Authen Flag = Dis, Mobile Tag = Dis,
SAA Profile = -, Ingress BW = -, Egress BW = -, Ingress Depth = -, Egress Depth = -,
Inact Interval = 10, Mac-Mobility = Dis

Total Profile Count: 3

-> show unp profile unp1-vlan
Profile Name: unp1-vlan
Qos Policy = -, Location Policy = loclist1,
Period Policy = timelist1, CP Profile = guest-profile,
CP State = Dis, Authen Flag = Dis, Mobile Tag = Dis,
SAA Profile = -, Ingress BW = -, Egress BW = -, Ingress Depth = -, Egress Depth = -,
Inact Interval = 10, Mac-Mobility = Dis, Kerberos Auth = Dis
<table>
<thead>
<tr>
<th>Output Definitions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile Name</strong></td>
<td>The name of the UNP profile. Configured through the <code>unp profile</code> command.</td>
</tr>
<tr>
<td><strong>QoS Policy</strong></td>
<td>The name of the QoS policy list associated with the profile. Configured through the <code>unp profile qos-policy-list</code> command.</td>
</tr>
<tr>
<td><strong>Location Policy</strong></td>
<td>The name of the location policy assigned to the UNP profile. Configured through the <code>unp profile location-policy</code> command.</td>
</tr>
<tr>
<td><strong>Period Policy</strong></td>
<td>The name of the period policy assigned to the UNP profile. Configured through the <code>unp profile period-policy</code> command.</td>
</tr>
<tr>
<td><strong>CP Profile</strong></td>
<td>The name of the Captive Portal (CP) profile assigned to the UNP profile. A CP profile defines a CP configuration that is applied to devices when CP authentication is enabled for the UNP profile. Configured through the <code>unp profile captive-portal-profile</code> command.</td>
</tr>
<tr>
<td><strong>CP State</strong></td>
<td>The CP authentication status (Ena or Dis) for the UNP profile. Indicates whether CP authentication is triggered for devices classified into the profile. Configured through the <code>unp profile captive-portal-authentication</code> command.</td>
</tr>
<tr>
<td><strong>Authen Flag</strong></td>
<td>The authentication flag status (Ena or Dis) for the UNP profile. Indicates whether only authenticated devices are allowed into the profile. Configured through the <code>unp profile authentication-flag</code> command.</td>
</tr>
<tr>
<td><strong>Mobile Tag</strong></td>
<td>The mobile tag status (Ena or Dis) for the UNP profile. When enabled, the first user that is learned on a UNP port and is classified into a UNP profile will cause the UNP port to be added as a tagged member of the VLAN associated with the profile. If the profile is mapped to a service, a tagged virtual port association is created. Configured through the <code>unp profile mobile-tag</code> command.</td>
</tr>
<tr>
<td><strong>SAA Profile</strong></td>
<td>The name of a Service Assurance Agent (SAA) profile that is associated with the UNP profile. Configured through the <code>unp profile saa-profile</code> command.</td>
</tr>
<tr>
<td><strong>Ingress BW</strong></td>
<td>The maximum ingress bandwidth setting that is applied to ports associated with the profile. Configured through the <code>unp profile maximum-ingress-bandwidth</code> command.</td>
</tr>
<tr>
<td><strong>Egress BW</strong></td>
<td>The maximum egress bandwidth setting that is applied to ports associated with the profile. Configured through the <code>unp profile maximum-egress-bandwidth</code> command.</td>
</tr>
<tr>
<td><strong>Ingress Depth</strong></td>
<td>The maximum ingress depth setting that is applied to ports associated with the profile. Configured through the <code>unp profile maximum-ingress-depth</code> command.</td>
</tr>
<tr>
<td><strong>Egress Depth</strong></td>
<td>The maximum egress depth setting that is applied to ports associated with the profile. Configured through the <code>unp profile maximum-egress-depth</code> command.</td>
</tr>
<tr>
<td><strong>Inact Interval</strong></td>
<td>The amount of time, in seconds, that a device can remain inactive after the MAC address for the device has aged out. When the timer reaches this value, inactive devices are automatically logged out of the network. Configured through the <code>unp profile inactivity-interval</code> command.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac-Mobility</td>
<td>The status of MAC address mobility (Ena or Dis) for the UNP profile. MAC mobility functionality applies only to profiles that are mapped to SPB services and is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M. Configured through the <code>unp profile mac-mobility</code> command.</td>
</tr>
<tr>
<td>Kerberos Auth</td>
<td>The status of Kerberos snooping (Ena or Dis) for the UNP profile. Indicates whether Kerberos snooping authentication is triggered for devices classified into the profile. Configured through the <code>unp profile kerberos-authentication</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command was introduced.
Release 8.4.1.R02; the built-in “defaultWLANProfile” included in the display.
Release 8.4.1.R03; “Redirect State” field deprecated.
Release 8.5R2; default UNP profiles for Device Profiling included in the display.
Release 8.6R1; “Mac-Mobility” field added.
Release 8.6R2; “Kerberos Auth” field added.

Related Commands

- `show unp classification` Displays the UNP classification rule configuration for the switch.
- `show unp global configuration` Displays the UNP global parameter values configured for the switch.
- `show unp port` Displays the UNP configuration for the port.
- `show unp user` Displays information about the devices learned on a UNP port.

MIB Objects

- `alaDaUNPProfileTable`
  - `alaDaUNPProfileName`
  - `alaDaUNPProfileAuthenticationFlag`
  - `alaDaUNPProfileMobileTag`
  - `alaDaUNPProfileCPortalAuthentication`
  - `alaDaUNPProfileRedirect`
  - `alaDaUNPProfileQoSPolicy`
  - `alaDaUNPProfilePeriodPolicy`
  - `alaDaUNPProfileCPortalProfile`
  - `alaDaUNPProfileLocationPolicy`
  - `alaDaUNPProfileSaaProfile`
  - `alaDaUNPProfileInactivityInterval`
  - `alaDaUNPProfileMaxIngressBandwidth`
  - `alaDaUNPProfileMaxEgressBandwidth`
  - `alaDaUNPProfileMaxIngressDepth`
  - `alaDaUNPProfileMaxEgressDepth`
  - `alaDaUNPProfileMacMobility`
  - `alaDaUNPProfileKerberosAuthentication`
show unp profile map

Displays the VLAN, service, or L2 GRE tunnel mapping configuration assigned to a UNP profile.

```
show unp profile [profile_name] map {vlan | service-type {spb | vxlan | static | l2gre}}
```

### Syntax Definitions

- **profile_name**: The name of the UNP to display.
- **vlan**: Displays the VLAN mapping configuration for a UNP profile.
- **spb**: Displays the Shortest Path Bridging (SPB) service mapping configuration for a UNP profile.
- **vxlan**: Displays the Virtual eXtensible Local Area Network (VXLAN) service mapping configuration for a UNP profile.
- **static**: Displays the existing SPB or VXLAN service IDs that are statically assigned to a UNP profile. This type of mapping is used to map the profile to a known service ID.
- **l2gre**: Displays the L2 GRE tunnel mapping configuration for a UNP profile.

### Defaults

By default, the VLAN, service, or L2 GRE tunnel mapping configuration for all profiles is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter a UNP profile name with this command to display the mapping information for a specific profile.
- Only one VLAN or service is mapped to a profile at any given time.

### Examples

```
-> show unp profile map vlan
Profile Name      Vlan-Id
-------------------------
unp1-vlan        300
unp2-vlan        301
unp3-vlan        500
unp4-vlan        501

Total Profile Vlan-Map Count: 4
```
-> show unp profile unp2-vlan map vlan
Profile Name                         Vlan-Id
-----------------------------------+--------
unp2-vlan                           301

output definitions

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>The name of the UNP profile that is mapped to the VLAN ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan-Id</td>
<td>The VLAN ID associated with the profile.</td>
</tr>
</tbody>
</table>

-> show unp profile map service-type spb
Profile Name Isid Tag Value BVlan Xlation Mode Snoop Profile Snoop Profile Remove
Name Isid Value BVlan Xlation Mode Snoop Profile Snoop Profile
---------------------------------+--------+-----+-----+-------+-------+------+-------+------+
unp1-spb 1500 10 400 Ena Tandem Ena - Ena - Dis
unp2-spb 1600 20:30 401 Ena Headend Ena ipms-2 Dis - Dis
unp3-spb 1700 10 500 Dis Headend Dis - Dis - Ena
SystemDefault1000001 10000010 10 4000 Dis Headend Dis - Dis - Ena

Total Profile Spb-Map Count: 4

output definitions

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>The name of the UNP profile that is mapped to the SPB service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isid</td>
<td>The SPB service instance identifier (I-SID) that will be used to dynamically create the SPB service access point (SAP) for the profile.</td>
</tr>
<tr>
<td>Tag Value</td>
<td>The VLAN ID tags of the traffic that the dynamically created SPB SAP will carry for the profile.</td>
</tr>
<tr>
<td>BVlan</td>
<td>The SPB BVLAN ID that will be associated with the I-SID for the dynamically created SPB SAP.</td>
</tr>
<tr>
<td>Vlan Xlation</td>
<td>The status of egress VLAN translation (Ena or Dis) for the dynamically created SPB SAP.</td>
</tr>
<tr>
<td>Mcast Mode</td>
<td>The multicast mode (Headend or Tandem) for the dynamically created SPB SAP.</td>
</tr>
<tr>
<td>Igmp Snoop</td>
<td>The status of IGMP snooping for the dynamically created SPB SAP.</td>
</tr>
<tr>
<td>Igmp Profile</td>
<td>The name of the optional IPMS profile that is applied to the IGMP snooping instance for the dynamically created SPB SAP.</td>
</tr>
<tr>
<td>Mld Snoop</td>
<td>The status of MLD snooping for the dynamically created SPB SAP.</td>
</tr>
<tr>
<td>Mld Profile</td>
<td>The name of the optional MLD profile that is applied to the IGMP snooping instance for the dynamically created SPB SAP.</td>
</tr>
<tr>
<td>Remove IngTag</td>
<td>Whether the customer VLAN tag is removed before the packet is encapsulated for the dynamically created SPB SAP (Ena or Dis).</td>
</tr>
</tbody>
</table>

-> show unp profile map service-type vxlan
Profile Name Vnid Value Far-End-List Vlan Mcast Mcast Mac Remove
Name Vnid Value Far-End-List Vlan Mcast Mcast Mac Remove
----------------------------------+--------+-------+------------+--------+-------+----------+-------+------+
vxlan1 1 0 Ena Hybrid 224.0.0.10 Ena Dis
vxlan2 2 0 Ena Hybrid 224.0.0.10 Ena Dis

Total Profile Vxlan-Map Count: 2
output definitions

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>The name of the UNP profile that is mapped to the VXLAN service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vnid</td>
<td>The VXLAN network identifier for the VXLAN segment that will be used to dynamically create the VXLAN service access point (SAP) for the profile.</td>
</tr>
<tr>
<td>Tag Value</td>
<td>The VLAN ID tags of the traffic that the dynamically created VXLAN SAP will carry for the profile.</td>
</tr>
<tr>
<td>Far-End-List</td>
<td>The name of the list that contains the IP addresses for the far-end VXLAN Tunnel End Points (VTEPs). The VTEPs are used to create Service Distribution Points (SDPs) for the dynamically created VXLAN SAP.</td>
</tr>
<tr>
<td>Vlan Xlation</td>
<td>The status of egress VLAN translation (Ena or Dis) for the dynamically created VXLAN SAP.</td>
</tr>
<tr>
<td>Mcast Mode</td>
<td>The multicast mode (Headend, Tandem, or Hybrid) for the dynamically created VXLAN SAP.</td>
</tr>
<tr>
<td>Mcast Group</td>
<td>The multicast group IP address that the dynamically created VXLAN SAP will use to forward traffic to participating VTEPs.</td>
</tr>
<tr>
<td>Mac Orchest</td>
<td>The status of Mac Orchestration (Ena or Dis) for the dynamically created VXLAN SAP. This parameter is automatically configured through OmniSwitch integration with Open vSwitch Database (OVSD) protocols. See the &quot;Web Services, CLI Scripting, OpenFlow, and AOS Micro Services (AMS)&quot; chapter in the OmniSwitch AOS Release 8 Switch Management Guide for more information.</td>
</tr>
<tr>
<td>Remove IngTag</td>
<td>Whether the customer VLAN tag is removed before the packet is encapsulated for the dynamically created VXLAN SAP (Ena or Dis).</td>
</tr>
</tbody>
</table>

-> show unp profile map service-type l2gre
Profile Name   Tag   Far-End-List Far-End-Ip Port  Vlan  Remove
Name           Vnid  Value          Isolation Xlation IngTag
-------------------------------+-------+--------+------------------+
guest-profile  2002  20            20.2.2.1   Ena  Dis  Ena

Total Profile L2gre-Map Count: 1

output definitions

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>The name of the UNP profile that is mapped to the L2 GRE tunnel.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vnid</td>
<td>The tunnel ID that identifies a GRE tunnel VPN.</td>
</tr>
<tr>
<td>Tag Value</td>
<td>The VLAN ID tags of the traffic that the dynamically created L2 GRE SAP will carry for the profile.</td>
</tr>
<tr>
<td>Far-End-List</td>
<td>The name of the list that contains the Loopback0 IP interface address for the far-end tunnel aggregation switch.</td>
</tr>
<tr>
<td>Far-End-Ip</td>
<td>The Loopback0 IP interface address for the far-end tunnel aggregation switch.</td>
</tr>
<tr>
<td>Port Isolation</td>
<td>The status of port isolation for the dynamically created L2 GRE SAP. Port isolation is implicitly enabled and is not configurable in this release.</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 40-341
output definitions

<table>
<thead>
<tr>
<th>Vlan Xlation</th>
<th>The status of VLAN translation (<strong>Ena</strong> or <strong>Dis</strong>) for the dynamically created L2 GRE SAP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove IngTag</td>
<td>Whether the customer VLAN tag is removed before the packet is encapsulated for the dynamically created L2 GRE SAP (<strong>Ena</strong> or <strong>Dis</strong>).</td>
</tr>
</tbody>
</table>

`-> show unp profile map service-type static
Profile                                   Tag
Name                             SvcId    Value
--------------------------------+--------+--------
unp1-staticSPB                   10       20
unp2-staticVXLAN                 20       40:50
Total Profile Static-Service-Map Count: 2

output definitions

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>The name of the UNP profile that is mapped to the static service.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SvcId</td>
<td>The service ID for the existing SPB or VXLAN service.</td>
</tr>
<tr>
<td>Tag Value</td>
<td>The VLAN ID tags of the traffic that the SAP associated with the service ID will carry.</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command was introduced.
Release 8.4.1.R02; **l2gre** parameter added.
Release 8.6R1; IGMP and MLD snooping related fields added to SPB service-mapped profile display; “Port-Isolation” and “Vlan Xlation” fields added to L2 GRE service-mapped profile display.
Release 8.7R1; “Mac Orchest” field added to VXLAN service-mapped profile display.
Release 8.7R2; “Remove IngTag” field added to the service-mapped profile display for SPB, VXLAN, and L2 GRE.

Related Commands

- **unp profile map vlan**
  - Configures the mapping of a standard VLAN to a UNP profile.

- **unp profile map service-type spb**
  - Configures the mapping of SPB parameters that are used to dynamically create an SPB SAP to carry profile traffic.

- **unp profile map service-type vxlan**
  - Configures the mapping of VXLAN parameters that are used to dynamically create a VXLAN SAP to carry profile traffic.

- **unp profile map service-type l2gre**
  - Configures the mapping of L2 GRE tunnel parameters that are used to dynamically create an L2 GRE tunnel SAP to carry profile traffic.

- **unp profile map service-type static**
  - Configures the mapping of an existing SPB or VXLAN service to the profile.

- **show unp profile**
  - Displays the UNP profile configuration for the switch.

- **show unp vxlan far-end-ip-list**
  - Displays the contents of a far-end IP address list that is used to map VXLAN service parameters to a profile.

- **show unp l2gre far-end-ip-list**
  - Displays the contents of a far-end IP address list that is used to map L2 GRE service parameters to a profile.
**MIB Objects**

alaDaUNPProfileTable
   alaDaUNPProfileName
alaDaUNPProfileMapVlanTable
   alaDaUNPProfileMapVlanVlanID
alaDaUNPProfileMapSpbTable
   alaDaUNPProfileMapSpbEncapVal
   alaDaUNPProfileMapSpbIsid
   alaDaUNPProfileMapSpbBVlan
   alaDaUNPProfileMapSpbMulticastMode
   alaDaUNPProfileMapSpbVlanXlation
   alaDaUNPProfileMapSpbIgmpSnooping
   alaDaUNPProfileMapSpbIgmpProfile
   alaDaUNPProfileMapSpbMldSnooping
   alaDaUNPProfileMapSpbMldProfile
   alaDaUNPProfileMapSpbRemoveIngressTag
alaDaUNPProfileMapVxlanTable
   alaDaUNPProfileMapVxlanEncapVal
   alaDaUNPProfileMapVxlanVnid
   alaDaUNPProfileMapVxlanFarEndIPList
   alaDaUNPProfileMapVxlanMulticastIPAddressType
   alaDaUNPProfileMapVxlanMulticastIPAddress
   alaDaUNPProfileMapVxlanVlanXlation
   alaDaUNPProfileMapVxlanMulticastMode
   alaDaUNPProfileMapVxlanMacOrchestration
   alaDaUNPProfileMapVxlanRemoveIngressTag
alaDaUNPProfileMapL2GreTable
   alaDaUNPProfileMapL2GreEncapVal
   alaDaUNPProfileMapL2GreVpnid
   alaDaUNPProfileMapL2GreFarEndIPAddressType
   alaDaUNPProfileMapL2GreFarEndIPAddress
   alaDaUNPProfileMapL2GreFarEndIPList
   alaDaUNPProfileMapL2GrePortIsolation
   alaDaUNPProfileMapL2GreVlanXlation
   alaDaUNPProfileMapL2GreRemoveIngressTag
alaDaUNPProfileMapStaticTable
   alaDaUNPProfileMapStaticEncapVal
   alaDaUNPProfileMapStaticServiceID
show unp vxlan far-end-ip-list

Displays the contents of an IP address list. Each address represents a VXLAN Tunnel End Point (VTEP). A far-end IP list is associated with a VXLAN service to identify all the VTEPs that will participate in that service.

show unp vxlan far-end-ip-list [ip_list_name]

Syntax Definitions

`ip_list_name`  
The name of a list that contains the IP addresses for the far-end VTEPs.

Defaults

By default, the contents of all the VXLAN far-end IP address lists is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72/Q32</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enter a list name with this command to display information for a specific list.

Examples

```
-> show unp vxlan far-end-ip-list
Far-End-Ip-List Name: toDataCenter1, IP-Count: 3,  
  IP-Addresses:  
    101.1.1.1  
    102.1.1.1  
    103.1.1.1  
Far-End-Ip-List Name: toDataCenter2, IP-Count: 3,  
  IP-Addresses:  
    201.1.1.1  
    202.1.1.1  
    203.1.1.1  

-> show unp vxlan far-end-ip-list toDataCenter2
Far-End-Ip-List Name: toDataCenter2, IP-Count: 3,  
  IP-Addresses:  
    201.1.1.1  
    202.1.1.1  
    203.1.1.1  
```
**Output Definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Far-End-Ip-List Name</td>
<td>The name of the far-end IP address list.</td>
</tr>
<tr>
<td>IP-Count</td>
<td>The number of IP addresses in the list.</td>
</tr>
<tr>
<td>IP-Addresses</td>
<td>The IP addresses that are members of the specified list name.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `unp vxlan far-end-ip-list` Configures a UNP VXLAN far-end IP list.
- `show unp profile map` Displays the VXLAN service profile mapping configuration for the switch.

**MIB Objects**

- `alaDaUNPVxlanFarEndIPListTable`  
  - `alaDaUNPVxlanFarEndIPListName`  
  - `alaDaUNPVxlanFarEndIPListIPAddressCount`
show unp l2gre far-end-ip-list

Displays the contents of an IP address list that contains the IP address of the Loopback0 interface configured on the far-end tunnel aggregation switch.

show unp l2gre far-end-ip-list [ip_list_name]

Syntax Definitions

ip_list_name

The name of a list that contains the IP address for the far-end tunnel aggregation switch.

Defaults

By default, the contents of all the far-end IP address lists is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enter a list name with this command to display information for a specific list.

Examples

-> show unp l2gre far-end-ip-list
Far-End-Ip-List Name: toDataCenter1, IP-Count: 1, IP-Addresses:
    100.1.1.1
Far-End-Ip-List Name: toDataCenter2, IP-Count: 1, IP-Addresses:
    202.1.1.1

-> show unp l2gre far-end-ip-list toDataCenter2
Far-End-Ip-List Name: toDataCenter2, IP-Count: 1, IP-Addresses:
    202.1.1.1

output definitions

<table>
<thead>
<tr>
<th>Far-End-Ip-List Name</th>
<th>The name of the far-end IP address list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-Count</td>
<td>The number of IP addresses in the list.</td>
</tr>
<tr>
<td>IP-Addresses</td>
<td>The IP address that is a member of the specified list name.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.5R2; command was introduced.

**Related Commands**

unp l2gre far-end-ip-list  Configures an L2 GRE far-end IP list.
show unp profile map  Displays the L2 GRE service profile mapping configuration for the switch.

**MIB Objects**

alaDaUNPL2GreFarEndIPListTable
  alaDaUNPL2GreFarEndIPListName
  alaDaUNPL2GreFarEndIPListIPAddressCount
show unp saa-profile

Displays the Service Assurance Agent (SAA) performance monitoring profile configuration for the switch. SAA profiles are assigned to UNP VLAN profiles to specify jitter and latency threshold values for SAA sessions that apply to the assigned UNP VLAN profile.

show unp saa-profile [profile_name]

Syntax Definitions

profile_name

The name of an existing SAA profile to display.

Defaults

By default, all SAA profiles are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Enter an SAA profile name with this command to display information for a specific profile.
- This command does not provide the UNP assignment for each SAA profile. Use the show unp profile command to display the assignment information.

Examples

```
-> show unp saa-profile
Profile Name | Latency Threshold | Jitter Threshold | MC Conf Status
-------------|-------------------|-----------------|---------------
unp_saa1     | 500               | 100             | Local
unp_saa2     | 0                 | 150             | Local
unp_saa3     | 250               | 0               | Local
```

output definitions

- **Profile Name**: The name of the SAA profile.
- **Latency Threshold**: The latency threshold value applied with this profile. A value of “0” indicates no threshold value is applied.
**output definitions**

<table>
<thead>
<tr>
<th>Jitter Threshold</th>
<th>The jitter threshold value applied with this profile. A value of “0” indicates no threshold value is applied.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC Conf Status</td>
<td>The MCLAG consistency check status of the UNP configuration (Sync, Out-Of-Sync, or Local). Note that MCLAG is not supported in this release.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- `unp saa-profile` Configures SAA performance monitoring profiles.
- `show unp profile` Displays the UNP profile configuration for the switch.

**MIB Objects**

- `alaDaSaaSProfileTable`
  - `alaDaSaaSProfileName`
  - `alaDaSaaSProfileLatencyThreshold`
  - `alaDaSaaSProfileJitterThreshold`
  - `alaDaSaaSProfileRowStatus`
show unp global configuration

Displays the switch configuration for the global Universal Network Profile (UNP) parameter settings.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- UNP global parameter settings determine specific actions related to the following:
  - Dynamically creating VLANs and/or profiles.
  - Whether or not devices attempting to authenticate are assigned to a temporary profile if the authentication server is unreachable.
  - Interaction with the Unified Policy Access Manager (UPAM) or the ClearPass Policy Manager (CPPM) as part of the OmniSwitch Bring Your Own Devices (BYOD) solution.
- A hyphen, “-”, indicates that a value has not been configured for the global UNP parameter.

Examples

-> show unp global configuration
  Dynamic Vlan Configuration = Disabled,
  Dynamic Profile Configuration = Disabled,
  Auth Server Down Profile1 = -,
  Auth Server Down Profile2 = -,
  Auth Server Down Profile3 = -,
  Auth Server Down Voice Profile1 = ALE_phones,
  Auth Server Down Voice Profile2 = IP_Phone,
  Auth Server Down Voice Profile3 = -,
  Auth Server Down Port Bounce = Disabled
  Auth Server Down Timeout = 60,
  Redirect Port Bounce = Enabled,
  Redirect Pause Timer = -
  Redirect http proxy-port = 8080
  Redirect Server FQDN = cppm.abc.com
Redirect Server IP = 10.135.20.50
Allowed IP = -
Force L3-Learning = Disabled
Force L3-Learning Port Bounce = Enabled
802.1x Pass Through Mode = Disabled
AP Mode = Enabled
Secure AP Mode = Disabled
System-default service-mod = 512
System-default service-base = 10000000
System-default Multicast-Mode = Headend
System-default Vlan-Xlation = Enabled
System-default Multicast-Group = 239.0.0.0
System-default far-end-ip-list = -
IPv6 Drop Packets = Disabled,
Delayed Learning Interval = 0,
Global Mac-Mobility = Disabled,
802.1x EAP Version = v3
Multiple Untag SAP = Enabled

output definitions

<table>
<thead>
<tr>
<th>Dynamic Vlan Configuration</th>
<th>The status (Enabled or Disabled) of dynamic VLAN configuration. Configured through the <code>unp dynamic-vlan-configuration</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Profile Configuration</td>
<td>The status (Enabled or Disabled) of dynamic profile configuration. Configured through the <code>unp dynamic-profile-configuration</code> command.</td>
</tr>
<tr>
<td>Auth Server Down Profile1</td>
<td>The name of a UNP that a device is assigned to in the event the RADIUS server is unreachable. Up to three different profile names are configurable as authentication server down UNP profiles. Configured through the <code>unp auth-server-down</code> command.</td>
</tr>
<tr>
<td>Auth Server Down Profile2</td>
<td></td>
</tr>
<tr>
<td>Auth Server Down Profile3</td>
<td></td>
</tr>
<tr>
<td>Auth Server Down Voice Profile1</td>
<td></td>
</tr>
<tr>
<td>Auth Server Down Voice Profile2</td>
<td></td>
</tr>
<tr>
<td>Auth Server Down Voice Profile3</td>
<td></td>
</tr>
<tr>
<td>Auth Server Down Port Bounce</td>
<td>The status (Enabled or Disabled) of the port-bounce feature for the authentication server down users globally on all the UNP ports. Configured through the <code>unp auth-server-down port-bounce</code> command.</td>
</tr>
<tr>
<td>Auth Server Down Timeout</td>
<td>The amount of time, in seconds, that devices remain assigned to the authentication server down UNP. Configured through the <code>unp auth-server-down-timeout</code> command.</td>
</tr>
<tr>
<td>Redirect Port Bounce</td>
<td>The status (Enabled or Disabled) of the port bounce operation for non-suppliant devices. Configured through the <code>unp redirect port-bounce</code> command.</td>
</tr>
<tr>
<td>Redirect Pause Timer</td>
<td>The amount of time, in seconds, the switch pauses to clear all device authentication states and trigger re-authentication. Configured through the <code>unp redirect pause-timer</code> command.</td>
</tr>
<tr>
<td>Redirect http proxy-port</td>
<td>The HTTP proxy port number to use for redirection to a server. Configured through the <code>unp redirect proxy-server-port</code> command.</td>
</tr>
<tr>
<td>Redirect Server FQDN</td>
<td>The Fully Qualified Domain Name of a redirection server. Configured through the <code>unp redirect server</code> command. This field is blank if an IP address was configured for the redirect server.</td>
</tr>
</tbody>
</table>
## output definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Configuration Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Redirect Server IP</strong></td>
<td>The IP network address of a redirection server. Configured through the <code>unp redirect server</code> command. If an FQDN was configured for the redirect server, then the resolved IP address for that domain will appear in this field.</td>
<td></td>
</tr>
<tr>
<td><strong>Allowed IP</strong></td>
<td>A list of IP addresses to which a host can access additional servers. Configured through the <code>unp redirect allowed-name</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Force L3-Learning</strong></td>
<td>The status (Enabled or Disabled) of UNP Layer 3 learning. Configured through the <code>unp force-l3-learning</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Force L3-Learning Port Bounce</strong></td>
<td>The status (Enabled or Disabled) of the port bounce action, which is associated with the Layer 3 learning function. Configured through the <code>unp force-l3-learning</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>802.1x Pass Through Mode</strong></td>
<td>Whether a supplicant device is authenticated locally (Enabled) or passed through to another switch for authentication (Disabled). Configured through the <code>unp 802.1x-pass-through</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>AP Mode</strong></td>
<td>The status (Enabled or Disabled) of the Access Point (AP) mode. This mode is enabled to support the detection of connected OmniAccess Stellar AP devices. Configured through the <code>unp ap-mode</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>System-default service-mod</strong></td>
<td>The modulo number that is used to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile. Configured through the <code>unp system-default service-mod</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>System-default service-base</strong></td>
<td>The base service number that is used to dynamically calculate an SPB I-SID value or a VXLAN VNID value for a System Default profile. Configured through the <code>unp system-default service-base</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>System-default Multicast-Mode</strong></td>
<td>The multicast replication mode (Headend or Tandem) for dynamic services that are created for System Default profiles. Configured through the <code>unp system-default multicastmode</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>System-default Vlan-Xlation</strong></td>
<td>The status (Enabled or Disabled) of VLAN translation for dynamic services that are created for System Default profiles. Configured through the <code>unp system-default vlan-xlation</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>System-default Multicast-Group</strong></td>
<td>The multicast group IP address for dynamic VXLAN services that are created for System Default profiles. Configured through the <code>unp system-default multicastgroup</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>System-default far-end-ip-list</strong></td>
<td>The name of a far-end IP list associated with dynamic VXLAN services that are created for System Default profiles. Configured through the <code>unp system-default far-end-ip-list</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>IPv6 Drop Packets</strong></td>
<td>The status (Enabled or Disabled) of IPv6 packet drop on UNP ports. Configured through the <code>unp ipv6-drop</code> command.</td>
<td></td>
</tr>
<tr>
<td><strong>Delayed Learning Interval</strong></td>
<td>The amount of time, in seconds, that UNP will wait before starting to learn packets received on UNP ports. Configured through the <code>unp delay-learning</code> command.</td>
<td></td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Global Mac-Mobility</th>
<th>The status (Enabled or Disabled) of MAC address mobility. The global status specifies the default status that is applied to new UNP profiles that are mapped to SPB service parameters. MAC mobility functionality is not supported on the OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6370M. Configured through the <strong>unp mac-mobility</strong> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x EAP Version</td>
<td>EAPOL version (V1 or V3) configured for 802.1x authentication. Configured through the <strong>unp 802.1x eapol-version</strong> command.</td>
</tr>
<tr>
<td>Multiple Untag SAP</td>
<td>Indicates whether multiple untagged user association for UNP dynamic SAP with different services is enabled or disabled.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.2.1; command was introduced.
Release 7.2.1.R02; “Dynamic Profile Configuration” and “MC Conf Status” fields added.
Release 7.3.4; “VXLAN” fields added; “MC Conf Status” fields deprecated.
Release 8.3.1.R02; “Force L3-Learning Port Bounce” field added.
Release 8.4.1.R02; “802.1x Pass Through Mode” and “AP Mode fields added”.
Release 8.5R1; “Redirect Server FQDN” and all of the “System-default” fields added.
Release 8.6R1; “Global Mac-Mobility” field added.
Release 8.7R1; “802.1x EAP Version” field added.
Release 8.9R1; “Multiple Untag SAP” field added.

**Related Commands**

- **show unp profile** Displays the UNP configuration for the switch.
- **show unp port** Displays the UNP configuration for the port.
- **show unp user** Displays information about the devices learned on a UNP port.

**MIB Objects**

alaDaUNPGlobalConfiguration
alaDaUNPDYNAMICVlanConfigFlag
alaDaUNPDYNAMICProfileConfigFlag
alaDaUNPAUTHServerDownProfile1
alaDaUNPAUTHServerDownProfile2
alaDaUNPAUTHServerDownProfile3
alaDaUNPAUTHServerDownTimeout
alaDaUNPRedirectPortBounce
alaDaUNPRedirectPauseTimer
alaDaUNPRedirectProxyServerPort
alaDaUNPRedirectServerIPTyp
alaDaUNPRedirectServerIP
alaDaUNPForceL3Learning
alaDaUNP8021XPpassThrough
alaDaUNPAPMode
alaDaUNPServiceModule
alaDaUNPServiceBase
alaDaUNPServiceMulticastMode
alaDaUNPServiceVlanXlation
alaDaUNPServiceMulticastGroup
alaDaUNPServiceFarEndIpList
alaDaUNPIPv6Drop
alaDaUNPDelayLearning
alaDaUNPMacMobility
alaDaUNPEapolVersion
alaDaUNPRedirectAllowedServerTable
  alaDaUNPRedirectAllowedServerIPType
  alaDaUNPRedirectAllowedServerIP
  alaDaUNPRedirectAllowedMaskIPType
  alaDaUNPRedirectAllowedMaskIP
show unp domain

Displays the UNP domain configuration for the switch.

show unp domain

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Domains are used to group physical UNP ports or link aggregates into one logical domain.
- Once a port is assigned to a specific domain, classification rules associated with the same domain ID are applied only to UNP ports associated with that same domain ID.

Examples

-> show unp domain

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Default-Domain</td>
</tr>
<tr>
<td>1</td>
<td>UNP Domain 1</td>
</tr>
<tr>
<td>2</td>
<td>UNP Domain 2</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command was introduced.
**Related Commands**

- **unp domain description**  
  Configures a domain ID to which UNP ports and classification rules are assigned.

- **unp domain**  
  Assigns a UNP port to a customer domain ID.

- **show unp port**  
  Displays the UNP configuration for the port.

**MIB Objects**

- `alaDaUnpCustomerDomainTable`
  - `alaDaUnpCustomerDomainId`
  - `alaDaUnpCustomerDomainDesc`
show unp classification

Displays the UNP classification rule configuration for the switch.

\texttt{show unp classification rule\_type}

---

\textbf{Syntax Definitions}

\begin{itemize}
  \item \textit{rule\_type} \quad The rule type to display (refer to the table in the “Usage Guidelines” section of this command page for a list of rule type parameters).
\end{itemize}

\textbf{Defaults}

N/A

\textbf{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\textbf{Usage Guidelines}

\begin{itemize}
  \item Specifying one of the following classification rule type parameters is required with this command:
    \begin{itemize}
      \item \texttt{mac-rule}
      \item \texttt{mac-domain-rule}
      \item \texttt{mac-oui-rule}
      \item \texttt{mac-range-rule}
      \item \texttt{mac-range-domain-rule}
      \item \texttt{ip-rule}
      \item \texttt{ip-domain-rule}
      \item \texttt{ip-range-rule}
      \item \texttt{vlan-tag-rule}
      \item \texttt{vlan-domain-rule}
      \item \texttt{port-rule}
      \item \texttt{domain}
      \item \texttt{authentication-type-rule}
      \item \texttt{lldp-rule}
    \end{itemize}
  \item Standard classification rule parameters are combined at the time a rule is created to define a binding classification rule. The parameter combinations provided with this command reflect the allowed binding rule parameter combinations.
  \item An extended classification rule defines a list of rules and allows more combinations of standard rules than the binding rule configuration (see the \texttt{show unp classification-rule} command).
\end{itemize}
### Examples

-> show unp classification mac-rule

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>VLAN Tag</th>
<th>Profile1 Name</th>
<th>Profile2 Name</th>
<th>Profile3 Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:2a:da:11:22:01</td>
<td>-</td>
<td>unp1-vlan</td>
<td>unp2-vxlan</td>
<td>unp3-vlan</td>
</tr>
<tr>
<td>00:0f:5b:46:d7:56</td>
<td>20</td>
<td>unp4-spb</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>00:2a:95:57:e1:67</td>
<td>-</td>
<td>unp2-vxlan</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Total Mac Rule Count: 3

-> show unp classification mac-range-rule

<table>
<thead>
<tr>
<th>Low MAC Address</th>
<th>High MAC Address</th>
<th>VLAN Tag</th>
<th>Profile1 Name</th>
<th>Profile2 Name</th>
<th>Profile3 Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:22:33:44:66</td>
<td>00:11:22:33:44:77</td>
<td>-</td>
<td>VNI-2400</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>00:11:22:33:44:88</td>
<td>00:11:22:33:44:99</td>
<td>10</td>
<td>CustB</td>
<td>VNP-B</td>
<td>-</td>
</tr>
</tbody>
</table>

Total Mac Range Rule Count: 2

-> show unp classification ip-rule

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Profile1 Name</th>
<th>Profile2 Name</th>
<th>Profile3 Name</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>255.255.255.0</td>
<td>unp1-vlan</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>20.0.0.1</td>
<td>255.255.255.0</td>
<td>CustA</td>
<td>VNI-2300</td>
<td>unp1-vlan</td>
<td>-</td>
</tr>
<tr>
<td>30.0.0.1</td>
<td>255.255.255.0</td>
<td>SLA-1</td>
<td>SLA-1525</td>
<td>-</td>
<td>50</td>
</tr>
</tbody>
</table>

Total IP Rule Count: 3

-> show unp classification mac-domain-rule

<table>
<thead>
<tr>
<th>Domain</th>
<th>MAC Address</th>
<th>Profile1 Name</th>
<th>Profile2 Name</th>
<th>Profile3 Name</th>
<th>Vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>00:22:da:00:9a:10</td>
<td>unp2-vxlan</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>00:2a:da:11:22:01</td>
<td>unp1-vlan</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

-> show unp classification mac-ip-port-rule

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>IP Address</th>
<th>Mask</th>
<th>Port</th>
<th>VLAN</th>
<th>Tag</th>
<th>Profile1 Name</th>
<th>Profile2 Name</th>
<th>Profile3 Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:2a:da:11:22:03</td>
<td>10.4.4.1</td>
<td>255.255.0.0</td>
<td>0/10</td>
<td>-</td>
<td>-</td>
<td>unp2-vxlan</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Total Mac-IP-Port Binding Rule Count: 1

-> show unp classification vlan-tag-rule

<table>
<thead>
<tr>
<th>VLAN Tag</th>
<th>Profile1 Name</th>
<th>Profile2 Name</th>
<th>Profile3 Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>unp3-vlan</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>10:20</td>
<td>unp1-vlan</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

-> show unp classification lldp-rule

<table>
<thead>
<tr>
<th>MED Endpoint</th>
<th>Profile1 Name</th>
<th>Profile2 Name</th>
<th>Profile3 Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-Phone</td>
<td>unp1-vlan</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Access-Point</td>
<td>defaultWLANProfile d</td>
<td>tefaultWLANAccessProfile</td>
<td>-</td>
</tr>
</tbody>
</table>

Total LLDP Rule Count: 2
output definitions

<table>
<thead>
<tr>
<th>Domain</th>
<th>The customer domain ID assigned to the classification rule for the specified profiles. The rule is applied to traffic received on UNP ports that are assigned to the same domain ID. This rule is also supported in combination with each of the other classification rules. Configured through the <strong>unp domain</strong> command or as a parameter with the other classification rule commands.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address value to match for this profile rule. Configured through the <strong>unp classification mac-address</strong> command.</td>
</tr>
<tr>
<td>Low MAC Address</td>
<td>The lowest and highest MAC address values used to specify a range of addresses to match for this rule. Configured through the <strong>unp classification mac-range</strong> command.</td>
</tr>
<tr>
<td>High MAC Address</td>
<td>The name of the UNP profile to which the rule is applied. Configured through the <strong>unp profile</strong> command.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP network address and mask values to match for this rule. Configured through the <strong>unp classification ip-address</strong> command.</td>
</tr>
<tr>
<td>Profile1, Profile2, Profile3</td>
<td>The MAC address value to match for this profile rule. Configured through the <strong>unp classification mac-address</strong> command.</td>
</tr>
<tr>
<td>VLAN Tag</td>
<td>The VLAN ID value to match for this profile rule.</td>
</tr>
<tr>
<td></td>
<td>- If one VLAN ID is displayed, the rule will match single-tagged packets or the outer VLAN tag of double-tagged packets.</td>
</tr>
<tr>
<td></td>
<td>- If two VLAN IDs are displayed, the rule will match double-tagged packets (for example, 10:20 will match outer VLAN tag 10 and inner VLAN tag 20).</td>
</tr>
<tr>
<td>MED Endpoint</td>
<td>The LLDP Media Endpoint Device to match for this profile rule (IP-Phone or Access-Point). Configured through the <strong>unp classification lldp med-endpoint</strong> command.</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command was introduced.

Related Commands

- **show unp classification-rule**: Displays the extended classification rule configuration for the switch.
- **show zeroconf server policy-instances**: Displays the UNP configuration for the switch.
- **show unp port**: Displays the UNP configuration for the port.
- **show unp user**: Displays information about the devices learned on a UNP port.

MIB Objects

| N/A |
**show unp classification-rule**

Displays the UNP extended classification rule configuration for the switch. An extended classification rule defines a list of rule conditions, all of which a device must match to be classified into the UNP profile associated with the extended rule name. A name and precedence value is also assigned to the list of rule conditions.

`show unp classification-rule [rule-name]`

### Syntax Definitions

*rule_name*  
The name of an existing extended classification rule.

### Defaults

By default, the configuration for all extended rules is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter the name of an extended classification rule to display information for a specific rule.
- An extended classification rule defines a list of rules and allows more combinations of standard rules than a binding rule configuration.
- An extended classification rule is associated with a UNP profile and applied to traffic learned on UNP ports.
- If Device Profiling is enabled for the switch, the following “built-in” extended classification rules are also displayed:
  - devProfPrinter
  - devProfWindows
  - devProfIP-Phone
  - devProfWireless-Router
  - devProfSmartPhone/PDA/Tablets

### Examples

```bash
-> show unp classification-rule
Rule Name: "ext_rule1"
  Precedence = 10,
```
Profile1 = unp1-vlan,
Conditions:
  Domain = 2,
  Mac-OUI = 00:22:11,
  VLAN Tag = 100

Rule Name: "ext_rule2"
  Precedence = 1,
  Profile1 = unp1-vlan,
  Profile2 = unp2-vxlan,
  Profile3 = unp3-vlan,
  Conditions:
    Domain = 20,
    Mac-Address = 00:2a:94:11:22:01,
    Port = 1/11,
    LLDP MED Endpoint = IP-Phone,
    Authentication-Type = None,

Rule Name: "devProfPrinter"
  Precedence = 255,
  Profile1 = devProfPrinter,
  Conditions:
    Device-Type = Printer,

Rule Name: "devProfWindows"
  Precedence = 255,
  Profile1 = devProfWindows,
  Conditions:
    Device-Type = Windows,

Rule Name: "devProfIP-Phone"
  Precedence = 255,
  Profile1 = devProfIP-Phone,
  Conditions:
    Device-Type = IP-Phone,

Rule Name: "devProfWireless-Router"
  Precedence = 255,
  Profile1 = devProfWireless-Router,
  Conditions:
    Device-Type = Wireless-Router,

Rule Name: "devProfSmartPhone/PDA/Tablets"
  Precedence = 255,
  Profile1 = devProfSmartPhone/PDA/Tablets,
  Conditions:
    Device-Type = Smartphone/PDA/Tablets,

Total Extended Classification Rule Count: 7

-> show unp classification-rule ext_rule2
Rule Name: "ext_rule2"
  Precedence = 1,
  Profile1 = unp1-vlan,
  Profile2 = unp2-vxlan,
  Profile3 = unp3-vlan,
  Conditions:
    Domain = 1,
    Mac-Address = 00:2a:94:11:22:01,
Port = 1/11,  
LLDP MED Endpoint = IP-Phone,  
Authentication-Type = None,  
-> show unp classification-rule devProfPrinter

Rule Name: "devProfPrinter"  
Precedence = 255,  
Profile1 = devProfPrinter,  
Conditions:  
Device-Type = Printer,

Release History

Release 8.1.1; command was introduced.  
Release 8.2.1; “VLAN Tag” field added.  
Release 8.3.1; “Edge-Profile” field replaced with “Profile1”, “Profile2”, and “Profile3” fields.  
Release 8.5R2; support added for displaying Device Profile extended classification rules.

Related Commands

unp classification-rule  
Configures an extended classification rule.

show unp classification  
Displays the standard classification rule configuration for the switch.

show unp profile  
Displays the UNP profile configuration for the switch.

MIB Objects

alaDaUNPClassifRuleTable  
alaDaUNPClassifRuleName  
alaDaUNPClassifRulePrecedenceNum  
alaDaUNPClassifRuleProfile1  
alaDaUNPClassifRuleProfile2  
alaDaUNPClassifRuleProfile3  
alaDaUNPClassifRulePort  
alaDaUNPClassifRulePortHigh  
alaDaUNPClassifRuleCustomerDomain  
alaDaUNPClassifRuleMacAddr  
alaDaUNPClassifRuleMacRngLoaddr  
alaDaUNPClassifRuleMacRngHiaddr  
alaDaUNPClassifRuleMacOuiAddr  
alaDaUNPClassifRuleEndPoin  
alaDaUNPClassifRuleAuthType  
alaDaUNPClassifRuleIpAddressType  
alaDaUNPClassifRuleIpAddress  
alaDaUNPClassifRuleIpMaskType  
alaDaUNPClassifRuleIpMask  
alaDaUNPClassifRuleVlanTag  
alaDaUNPClassifRuleDeviceType
**show unp user-role**

Displays the user-defined role configuration for the switch.

**show unp user-role [role_name]**

---

**Syntax Definitions**

*role_name*  
The name of an existing user-defined role.

---

**Defaults**

By default, all user-defined role are displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Enter a user-defined role name with this command to display information for a specific role.

---

**Examples**

```bash
-> show unp user-role
Role Name: ur1
  Qos Policy List       : qlist1
  Priority              : 1
  Conditions:
    Profile1            : unp1-vlan
    Profile2            : unp2-spb
    Profile3            : -
  Authentication-Type : Mac
  CP Status            : Enabled

Role Name: ur2
  Qos Policy List       : qlist-allow
  Priority              : 1
  Conditions:
    Profile1            : -
    Profile2            : -
    Profile3            : -
  Authentication-Type : 802.1x Fail
  CP Status            : Disabled

Total User Role Derivation Rule Count: 2
```

---
Access Guardian Commands

-> show unp user-role ur2

<table>
<thead>
<tr>
<th>Role Name</th>
<th>QoS Policy List Name</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>ur2</td>
<td>qlist-allow</td>
<td>1</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.1.1; command was introduced.
Release 8.3.1; “Edge-Profile” field replaced with “Profile1”, “Profile2”, and “Profile3” fields.

**Related Commands**

- **unp user-role**
  - Configures a user-defined role.
- **show unp user**
  - Displays information about devices learned on UNP ports.

**MIB Objects**

- alaDaUNPUserRoleTable
  - alaDaUNPUserRoleName
  - alaDaUNPUserRolePrecedenceNum
  - alaDaUNPUserRolePolicyList
  - alaDaUNPUserRoleProfile1
  - alaDaUNPUserRoleProfile2
  - alaDaUNPUserRoleProfile3
  - alaDaUNPUserRoleAuthType
  - alaDaUNPUserRolePostLoginStatus
**show unp restricted-role**

Displays the names of the explicit QoS policy lists assigned to the built-in restricted role states (Captive Portal pre-login, Unauthorized, and QMR) used by the switch.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X48C4E/V48C8/</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V32E/T24C2/</td>
<td>C32E/T24C2/</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An explicit QoS policy list overrides the built-in policy list associated with the restricted role state. When the explicit policy list assignment is removed, the switch reverts back to using the built-in policy list associated with the restricted role state.

**Examples**

-> show unp restricted-role

Role name  QoS Policy List Name
-------------------------------------------------------------
UNAUTHORIZED qlist-bad
QMR qlist-qmr
CP PRE-LOGIN qlist-cp

Total Restricted Role Count: 3

**output definitions**

<table>
<thead>
<tr>
<th>Role Name</th>
<th>The restricted role name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS Policy List</td>
<td>The name of the QoS policy list associated with the restricted role name.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.1.1; command was introduced.
Related Commands

- **unp restricted-role policy-list**: Configures a user-defined role.
- **show unp user**: Displays information about devices learned on UNP ports.

MIB Objects

- **alaDaUNPstrictedRoleTable**
  - **alaDaUNPstrictedRoleType**
  - **alaDaUNPstrictedRolePolicyList**
**show unp port**

Displays the UNP configuration for the port. Includes only ports and link aggregates on which UNP is enabled.

```plaintext
show unp {port [chassis/slot/port1[-port2]] | linkagg [agg_id[-agg_id2]]} [type {bridge | access}]
```

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` Link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (10-15).
- `bridge` Displays only UNP bridge ports.
- `access` Displays only UNP access ports.

---

**Defaults**

By default, configuration information for all UNP ports or link aggregates is displayed.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Enter a port or link aggregate ID number to display information specific to the port or link aggregate.
- Specify a UNP port type (`bridge` or `access`) to display information only for that type of UNP port.

---

**Examples**

```
$ show unp port
Port  Port  Type  802.1x  Mac  Class.  Default  802.1X  MAC  Trust-Tag
Domain Auth  Auth  Pass-Alt  Pass-Alt
--------+--------+-----------------+-----------------+----------+----------+-----------------+----------+----------+
1/16    1 Bridge  Disabled  Disabled  Enabled  unp-1001  -  -  Disabled
1/17    0 Bridge  Disabled  Disabled  unp-1001  -  -  Disabled
1/18    0 Access  Disabled  Enabled  spb1001  -  -  Enabled
1/35    0 Access  Disabled  Disabled  -  -  -  Disabled
1/36    5 Bridge  Enabled  Enabled  Disabled  DefUnp  1XProf1  MacPAS  Enabled
1/37    5 Access  Enabled  Disabled  Enabled  -  1XProf2  -  Enabled
```

---

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 40-367
-> show unp port 1/17

<table>
<thead>
<tr>
<th>Port</th>
<th>Domain</th>
<th>Type</th>
<th>802.1x</th>
<th>Mac</th>
<th>Class.</th>
<th>Default</th>
<th>802.1X</th>
<th>MAC</th>
<th>Trust-Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td>0</td>
<td>Bridge</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Disabled</td>
<td>unp-1001</td>
<td>-</td>
<td>-</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

-> show unp linkagg type bridge

<table>
<thead>
<tr>
<th>LagID</th>
<th>Domain</th>
<th>Type</th>
<th>802.1x</th>
<th>Mac</th>
<th>Class.</th>
<th>Default</th>
<th>802.1X</th>
<th>MAC</th>
<th>Trust-Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1</td>
<td>Bridge</td>
<td>Disabled</td>
<td>Enabled</td>
<td>unp-1001</td>
<td>-</td>
<td>-</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>Bridge</td>
<td>Disabled</td>
<td>Disabled</td>
<td>unp-1001</td>
<td>-</td>
<td>-</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Port/LagID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Domain</td>
<td>The customer domain ID assigned to the UNP port. Traffic received on the port is classified with UNP profile rules that are assigned to the same domain ID. Configured through the <code>unp domain</code> command.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of UNP port (Bridge or Access). UNP bridge ports classify traffic into VLAN profiles; UNP access ports classify traffic into service profiles. Configured through the <code>unp port-type</code> command.</td>
</tr>
<tr>
<td>802.1x Auth</td>
<td>The status of 802.1X authentication (Enabled or Disabled) for the UNP port or link aggregate. Configured through the <code>unp 802.1x-authentication</code> command.</td>
</tr>
<tr>
<td>Mac Auth</td>
<td>The status of MAC authentication (Enabled or Disabled) for the UNP port or link aggregate. Configured through the <code>unp mac-authentication</code> command.</td>
</tr>
<tr>
<td>Class.</td>
<td>The status of classification (Enabled or Disabled) for the UNP port or link aggregate. Configured through the <code>unp classification</code> command.</td>
</tr>
<tr>
<td>Default</td>
<td>The name of the default UNP assigned to the port or link aggregate. Configured through the <code>unp default-profile</code> command.</td>
</tr>
<tr>
<td>802.1X Pass-Alt</td>
<td>The name of the 802.1X authentication pass alternate UNP assigned to the port or link aggregate. Configured through the <code>unp 802.1x-authentication pass-alternate</code> command.</td>
</tr>
<tr>
<td>MAC Pass-Alt</td>
<td>The name of the MAC authentication pass alternate UNP assigned to the port or link aggregate. Configured through the <code>unp mac-authentication pass-alternate</code> command.</td>
</tr>
<tr>
<td>Trust-Tag</td>
<td>The status of the trust VLAN tag option for the UNP port or link aggregate. Configured through the <code>unp trust-tag</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command was introduced.
Related Commands

- **show unp profile**
  Displays the UNP configuration for the switch.

- **show unp port config**
  Displays detailed configuration information for UNP ports and link aggregates.

- **show unp user**
  Displays information about the devices learned on a UNP port.

MIB Objects

- **alaDaUNPPortTable**
  - **alaDaUNPPortIfIndex**
  - **alaDaUNPPortDomainID**
  - **alaDaUNPPortType**
  - **alaDaUNPPort8021XAuthStatus**
  - **alaDaUNPPortMacAuthFlag**
  - **alaDaUNPPortClassificationFlag**
  - **alaDaUNPPortDefaultProfileName**
  - **alaDaUNPPortPassAltProfileName**
  - **alaDaUNPPortTrustTagStatus**
show unp port config

Displays detailed configuration information for UNP ports and link aggregates.

```
show unp {port [chassis/slot/port1[-port2]] | linkagg [agg_id[-agg_id2]]} config
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **agg_id[-agg_id2]**
  - Link aggregate ID. Use a hyphen to specify a range of link aggregates IDs (10-15).

### Defaults

By default, configuration information for all ports or link aggregates is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>6900 C32E/T24C2</th>
<th>6900 X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `port` or `linkagg` parameter to display information for a specific port or link aggregate ID.

### Examples

```
-> show unp port 1/1/10 config
Port  1/1/10
      Port-Type          = BRIDGE,
      Redirect Port Bounce = Disabled,
      802.1x authentication = Enabled,
      802.1x Pass Alternate Profile = -, 802.1x Bypass = Disabled,
      802.1x failure-policy = default,
      Mac-auth allow-eap = -,  Mac authentication = Enabled,
      Mac Pass Alternate Profile = -,  Classification = Enabled,
      Trust-tag = Enabled,
      Default Profile = -,  Port Domain Num = 0,
      AAA Profile = -,  Port Template = bridgeDefaultPortTemplate,
      Port Control Direction = Both,
```
Egress Flooding = Not Allowed,
Admin State = Enabled,
Dynamic Service = -,
PVLAN Port Type = -,
Force L3-Learning = Disabled,
Force L3-Learning Port Bounce = Enabled,
AP Mode = Enabled,
802.1x Parameters:
    Tx-Period = 30,
    Supp-Timeout = 30,
    Max-req = 2
L2 Profile = -,

-> show unp port 1/1/11 config
Port 1/1/11
    Port-Type = Access,
    802.1x authentication = Enabled,
    802.1x Pass Alternate Profile = -,
    802.1x Bypass = Disabled,
    802.1x failure-policy = default,
    Mac-auth allow-eap = -,
    Mac authentication = Enabled,
    Mac Pass Alternate Profile = -,
    Classification = Enabled,
    Trust-tag = Enabled,
    Default Profile = -,
    Port Domain Num = 0,
    AAA Profile = -,
    Port Template = accessDefaultPortTemplate,
    Admin State = Enabled,
    Dynamic Service = spb,
    PVLAN Port Type = -,
    Force L3-Learning = Disabled,
    Force L3-Learning Port Bounce = Enabled,
    AP Mode = -,
    802.1x Parameters:
        Tx-Period = 30,
        Supp-Timeout = 30,
        Max-req = 2
    L2 Profile = "unp-def-access-profile",

-> show unp linkagg 12 config
Linkagg ID 0/12
    Port-Type = Bridge,
    Redirect Port Bounce = Disabled,
    802.1x authentication = Enabled,
    802.1x Pass Alternate Profile = -,
    802.1x Bypass = Disabled,
    802.1x failure-policy = default,
    Mac-auth allow-eap = -,
    Mac authentication = Enabled,
    Mac Pass Alternate Profile = -,
    Classification = Enabled,
    Trust-tag = Enabled,
    Default Profile = -,
    Port Domain Num = 0,
    AAA Profile = -,
    Port Template = bridgeDefaultPortTemplate,
    Port Control Direction = Both,
Egress Flooding = Not Allowed,
Admin State = Enabled,
Dynamic Service = -,
Force L3-Learning = Disabled,
Force L3-Learning Port Bounce = Enabled,
AP Mode = Enabled,
802.1x Parameters:
  Tx-Period = 30,
  Supp-Timeout = 30,
  Max-reqmeout = 2
L2 Profile = -,

*output definitions*

<table>
<thead>
<tr>
<th>Port or Linkagg ID</th>
<th>The port or link aggregate on which UNP is enabled. Configured through the <code>unp port-type</code> command. A “0” indicates the port is a link aggregate (for example, 0/12 is link aggregate ID 12).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Type</td>
<td>The type of UNP port (Bridge or Access).</td>
</tr>
<tr>
<td>Redirect Port Bounce</td>
<td>The status of the port bounce operation (Enabled or Disabled) for the UNP port or link aggregate. Configured through the <code>unp redirect port-bounce</code> command. This field applies only to UNP bridge ports and link aggregates.</td>
</tr>
<tr>
<td>802.1x Authentication</td>
<td>The 802.1X authentication status (Enabled or Disabled) for the UNP port or link aggregate. Configured through the <code>unp 802.1x-authentication</code> command.</td>
</tr>
<tr>
<td>802.1x Pass Alternate Profile</td>
<td>The name of the 802.1X authentication pass alternate profile assigned to the port or link aggregate. Configured through the <code>unp 802.1x-authentication pass-alternate</code> command</td>
</tr>
<tr>
<td>802.1x Bypass</td>
<td>The status of 802.1X bypass (Enabled or Disabled).</td>
</tr>
<tr>
<td>802.1x failure-policy</td>
<td>Whether the switch attempts subsequent MAC authentication for a device after the initial 802.1X authentication process fails (default = no MAC authentication or <code>mac-authentication</code>). This parameter option only applies to a UNP port or link aggregate on which 802.1X authentication bypass is enabled. Configured through the <code>unp mac-authentication allow-eap</code> command.</td>
</tr>
<tr>
<td>Mac-auth allow-eap</td>
<td>Indicates the conditions under which 802.1X authentication is performed or bypassed based on the initial MAC authentication process (pass = MAC authentication passes, fail = if MAC authentication fails, noauth = no MAC authentication, or none = do not attempt 802.1X authentication). This parameter option only applies to a UNP port or link aggregate on which 802.1X authentication bypass is enabled. Configured through the <code>unp mac-authentication allow-eap</code> command.</td>
</tr>
<tr>
<td>Mac Authentication</td>
<td>The MAC authentication status (Enabled or Disabled) for the UNP port or link aggregate. Configured through the <code>unp mac-authentication</code> command.</td>
</tr>
<tr>
<td>Mac Pass Alternate Profile</td>
<td>The name of the MAC authentication pass alternate profile assigned to the port or link aggregate. Configured through the <code>unp mac-authentication pass-alternate</code> command.</td>
</tr>
<tr>
<td>Classification</td>
<td>The classification status (Enabled or Disabled) for the UNP port or link aggregate. Configured through the <code>unp classification</code> command.</td>
</tr>
<tr>
<td>Trust-Tag</td>
<td>The status of the trust VLAN tag option for the UNP port or link aggregate. Configured through the <code>unp trust-tag</code> command.</td>
</tr>
<tr>
<td><strong>output definitions</strong></td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Default Profile</strong></td>
<td>The name of the default UNP profile assigned to the UNP port or link aggregate. Configured through the <code>unp default-profile</code> command.</td>
</tr>
<tr>
<td><strong>Port Domain Name</strong></td>
<td>The domain ID number assigned to the UNP port or link aggregate. Configured through the <code>unp domain</code> command.</td>
</tr>
<tr>
<td><strong>AAA Profile</strong></td>
<td>The name of an AAA profile assigned to the UNP port or link aggregate. Configured through the <code>unp aaa-profile</code> command.</td>
</tr>
<tr>
<td><strong>Port Template</strong></td>
<td>The name of a port template assigned to the UNP port or link aggregate. A port template defines and saves UNP port configuration options (such as the type of authentication, classification status, a default profile). Configured through the <code>unp port-port-template</code> command.</td>
</tr>
<tr>
<td><strong>Port Control Direction</strong></td>
<td>Whether 802.1X access control is applied to ingress and egress traffic (<strong>both</strong>) or just ingress traffic (<strong>in</strong>). Configured through the <code>unp direction</code> command. This field applies only to UNP bridge ports and link aggregates.</td>
</tr>
<tr>
<td><strong>Egress Flooding</strong></td>
<td>Indicates whether egress broadcast, unknown unicast, and multicast traffic is blocked (<strong>Not Allowed</strong>) or unblocked (<strong>Allowed</strong>) on the UNP port. The value displayed in this field is based on the port control direction setting for the port (<strong>both</strong> = Not Allowed; <strong>in</strong> = Allowed). This field is displayed only for UNP bridge ports and link aggregates.</td>
</tr>
<tr>
<td><strong>Admin State</strong></td>
<td>The administrative status (<strong>Enabled</strong> or <strong>Disabled</strong>) for the UNP port or link aggregate. Configured through the <code>unp admin-state</code> command.</td>
</tr>
<tr>
<td><strong>Dynamic Service</strong></td>
<td>The type of dynamic service (<strong>vxlan</strong> or <strong>spb</strong>) to generate on the UNP port or link aggregate. Configured through the <code>unp dynamic-service</code> command. This field applies only to UNP access ports and link aggregates.</td>
</tr>
<tr>
<td><strong>PVLAN Port Type</strong></td>
<td>The Private VLAN (PVLAN) port type for the UNP port or link aggregate (<strong>promiscuous</strong>, <strong>isl</strong>, <strong>community</strong>, or <strong>isolated</strong>). This field is displayed only for UNP access ports, not link aggregates.</td>
</tr>
<tr>
<td><strong>Force L3-Learning</strong></td>
<td>The status of Layer 3 learning (<strong>Enabled</strong> or <strong>Disabled</strong>) for the UNP port or link aggregate. Configured through the <code>unp force-l3-learning</code> command.</td>
</tr>
<tr>
<td><strong>Force L3-Learning Port Bounce</strong></td>
<td>The status of the port bounce action, which is an optional parameter associated with the Layer 3 learning function. Configured through the <code>unp force-l3-learning</code> command.</td>
</tr>
<tr>
<td><strong>AP Mode</strong></td>
<td>The Access Point mode status (<strong>Enabled</strong> or <strong>Disabled</strong>) for the UNP port or link aggregate. Configured through the <code>unp port ap-mode</code> command.</td>
</tr>
<tr>
<td><strong>802.1x Tx-Period</strong></td>
<td>The amount of time, in seconds, before an EAP Request Identity is retransmitted. Configured through the <code>unp 802.1x-authentication tx-period</code> command.</td>
</tr>
<tr>
<td><strong>802.1x Supp-Timeout</strong></td>
<td>The amount of time, in seconds, the switch waits before timing out an 802.1X user (supplicant) that is attempting to authenticate. Configured through the <code>unp 802.1x-authentication supp-timeout</code> command.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.1x Max-Req</strong></td>
<td>The maximum number of times the switch will retransmit a request for authentication information. Configured through the <code>unp 802.1x-authentication max-req</code> command.</td>
</tr>
<tr>
<td><strong>L2 Profile</strong></td>
<td>The name of a Layer 2 profile that is assigned to the UNP port or link aggregate. Configured through the <code>unp l2-profile</code> command. This field applies only to UNP access ports and link aggregates.</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command was introduced.
Release 8.3.1.R02; “Force L3-Learning” and “Force L3-Learning Port Bounce” fields added.
Release 8.4.1; “L2 Profile” field added.
Release 8.6R1; “AP Mode” field added.

Related Commands

- `show unp port` Displays the UNP port configuration for the switch.
- `show unp profile` Displays the UNP configuration for the switch.
- `show unp user` Displays information about the devices learned on a UNP port.

MIB Objects

alaDaUNPPortTable
  - alaDaUNPPortIfIndex
  - alaDaUNPPortDefaultProfileName
  - alaDaUNPPortPassAltProfileName
  - alaDaUNPPortMacAuthFlag
  - alaDaUNPPortClassificationFlag
  - alaDaUNPPortTrustTagStatus
  - alaDaUNPPortType
  - alaDaUNPPort8021XAAuthStatus
  - alaDaUNPPort8021XTxPeriod
  - alaDaUNPPort8021XS suppTimeOut
  - alaDaUNPPort8021XMaxReq
  - alaDaUNPPortAaaProfile
  - alaDaUNPPortRedirectPortBounce
  - alaDaUNPPort8021XFailurePolicy
  - alaDaUNPPort8021XBypassStatus
  - alaDaUNPPortMacAllowEap
  - alaDaUNPPortAdminControlledDirections
  - alaDaUNPPortAdminControlledOperDirections
  - alaDaUNPPort8021XPassAltProfileName
  - alaDaUNPPortPortTemplateName
  - alaDaUNPPortDomainID
  - alaDaUNPPortAdminState
  - alaDaUNPPortDynamicService
  - alaDaUNPPortPVlanPortType
  - alaDaUNPPortL2Profile
  - alaDaUNPPortApMode

802.1x Max-Req

The maximum number of times the switch will retransmit a request for authentication information. Configured through the `unp 802.1x-authentication max-req` command.

L2 Profile

The name of a Layer 2 profile that is assigned to the UNP port or link aggregate. Configured through the `unp l2-profile` command. This field applies only to UNP access ports and link aggregates.
show unp port bandwidth

Displays the bandwidth parameter values applied to a UNP port or link aggregate. These values are optionally assigned through the UNP profile to which a UNP port is associated.

show unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} bandwidth

Syntax Definitions

chassis/slot/port1[-port2] The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).

agg_id[-agg_id2] Link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the port or linkagg parameter to display information for a specific port or link aggregate ID.

- Bandwidth parameter values are not applied to UNP link aggregates that are assigned to the profile. As a result, this command will always show the bandwidth parameter values as not set for link aggregates.

- The optional bandwidth parameter values are applied when a UNP port is classified into a UNP profile. The profile name is obtained through local classification or returned from the RADIUS server.

- The source from which the bandwidth parameter values was last updated is also included in the display information. The source updates are based on the following conditions:
  - The UNP profile applies the bandwidth values at the time the UNP port is classified into the profile. This overrides any existing QoS bandwidth policies configured on the physical port.
  - QoS bandwidth policies defined in a QoS policy list associated with the profile are applied after the port is classified into the profile. This overrides the profile bandwidth values initially applied.
  - User-configured QoS bandwidth policies are applied after the port is classified into the profile.
Examples

The following example shows the default display of UNP rate limit parameters when no users are learned on the UNP port:

```
-> show unp port 1/1/11 bandwidth
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Max Ingress Bandwidth</th>
<th>Ingress BW Source</th>
<th>Ingr BW Profile</th>
<th>Max Egress Bandwidth</th>
<th>Egress BW Source</th>
<th>Egress BW Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/11</td>
<td>Bridge</td>
<td>0</td>
<td></td>
<td>-</td>
<td>0</td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

The following example shows the UNP rate limit parameters that are applied when user devices are assigned to a UNP profile that specifies bandwidth parameter values:

```
-> show unp port 1/1/11 bandwidth
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Max Ingress Bandwidth</th>
<th>Ingress BW Source</th>
<th>Ingr BW Profile</th>
<th>Max Egress Bandwidth</th>
<th>Egress BW Source</th>
<th>Egress BW Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/11</td>
<td>Bridge</td>
<td>50.0M</td>
<td>UNP</td>
<td>Ingress50</td>
<td>30.0M</td>
<td>UNP</td>
<td>Egress30</td>
</tr>
</tbody>
</table>

The following example shows the rate limit parameter values that are applied when QoS policies override the bandwidth parameter values that were applied through UNP profile settings:

```
-> qos port 1/1/11 maximum ingress-bandwidth 60M maximum egress-bandwidth 60M
```

```
-> show unp port 1/1/11 bandwidth
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Max Ingress Bandwidth</th>
<th>Ingress BW Source</th>
<th>Ingr BW Profile</th>
<th>Max Egress Bandwidth</th>
<th>Egress BW Source</th>
<th>Egress BW Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/11</td>
<td>Bridge</td>
<td>60.0M</td>
<td>QoS</td>
<td>-</td>
<td>60.0M</td>
<td>QoS</td>
<td>-</td>
</tr>
</tbody>
</table>

output definitions

- **Port**: The port or link aggregate on which UNP is enabled. A “0” indicates the port is a link aggregate (for example, 0/11 is link aggregate ID 11). Configured through the `unp port-type` command.

- **Port Domain**: The domain ID assigned to the UNP port or link aggregate. Configured through the `unp domain` command.

- **Type**: The type of UNP port (Bridge or Access). Configured through the `unp port-type` command.

- **Max Ingress Bandwidth**: The maximum ingress bandwidth value applied to the UNP port. Configured through the `unp profile maximum-ingress-bandwidth` command.

- **Ingress BW Source**: The source from which the maximum ingress bandwidth value was updated on the port (UNP or QoS).

- **Ingr BW Profile**: The name of the UNP profile responsible for setting the maximum ingress bandwidth value on the UNP port. This field is only applicable when UNP classification applies the bandwidth setting on the port.

- **Max Egress Bandwidth**: The maximum egress bandwidth value applied to the UNP port. Configured through the `unp profile maximum-egress-bandwidth` command.

- **Egress BW Source**: The source from which the maximum egress bandwidth value was updated on the port (UNP or QoS).

- **Egress BW Profile**: The name of the UNP profile responsible for setting the maximum egress bandwidth value on the UNP port. This field is only applicable when UNP classification applies the bandwidth setting on the port.
output definitions

Max Ingress Depth
The maximum ingress depth value that is applied to the UNP port. This value determines how much the traffic can burst over the maximum ingress bandwidth rate. Configured through the `unp profile maximum-ingress-depth` command.

Max Egress Depth
The maximum egress depth value that is applied to the UNP port. This value determines how much the traffic can burst over the maximum egress bandwidth rate. Configured through the `unp profile maximum-egress-depth` command.

Release History
Release 8.2.1; command was introduced.

Related Commands
`show unp port` Displays the UNP port configuration for the switch.
`show unp profile` Displays the UNP profile configuration for the switch.

MIB Objects
alaDaUNPPortTable
alaDaUNPPortIfIndex
alaDaUNPPortDomainID
alaDaUNPPortType
alaDaUNPPortMaxIngressBw
alaDaUNPPortMaxIngressBwSource
alaDaUNPPortMaxEgressBw
alaDaUNPPortMaxEgressBwSource
alaDaUNPPortMaxIngressDepth
alaDaUNPPortMaxEgressDepth
alaDaUNPPortIngressSourceProfile
alaDaUNPPortEgressSourceProfile
show unp port 802.1x statistics

Displays 802.1X statistics for a UNP port or link aggregate on which 802.1X authentication is enabled.

show unp {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]} 802.1x statistics

Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: Link aggregate ID. Use a hyphen to specify a range of link aggregates IDs (10-15).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the **port** or **linkagg** parameter to display information for a specific UNP port or link aggregate ID.

Examples

-> show unp port 1/1/13 802.1x statistics
Port 1/1
Mac-address=00:00:00:00:00:01,
Vlan=0,
Rx EAP Frames=0,
Tx EAP Frames=0,
Rx EAP Logoff Frames=0,
Tx EAP Request Frames=0,
Tx EAP Request ID Frames=0,
Rx EAP Response Frames=0,
Rx EAP Response ID Frames=0,
Rx EAP Start Frames=0,
Rx Invalid EAP Frames=0,
Rx Length Error EAP Frames=0,
Last EAP Frame Version=0,
Last EAP Frame Version=0,
Last EAP Source=00:00:00:00:00:00
Access Guardian Commands

show unp port 802.1x statistics

-> show unp linkagg 20 802.1x statistics
Linkagg ID 0/10
  Mac-address=00:00:00:00:00:01,
  Vlan=0,
  Rx EAP Frames=0,
  Tx EAP Frames=0,
  Rx EAP Logoff Frames=0,
  Tx EAP Request Frames=0,
  Tx EAP Request ID Frames=0,
  Rx EAP Response Frames=0,
  Rx EAP Response ID Frames=0,
  Rx EAP Start Frames=0,
  Rx Invalid EAP Frames=0,
  Rx Length Error EAP Frames=0,
  Last EAP Frame Version=0,
  Last EAP Frame Version=0,
  Last EAP Source=00:00:00:00:00:00

Release History

Release 7.3.4; command was introduced.

Related Commands

show unp port Displays the UNP port configuration for the switch.
show unp user Displays information about the devices learned on a UNP port.

MIB Objects

N/A
show unp port configured-vlans

Displays the VLANs assigned to UNP bridge ports or link aggregates.

show unp {port [chassis/slot/port1[-port2]] | linkagg [agg_id1-agg_id2]} configured-vlans

Syntax Definitions

chassis/slot/port1[-port2] The chassis ID, slot, and port number (3/1/1) for a specific UNP bridge port. Use a hyphen to specify a range of ports (3/1/1-8).

agg_id1-agg_id2 Link aggregate ID for a specific UNP bridge link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the port or linkagg parameter to display information for a specific UNP bridge port or link aggregate ID.
- If the port or linkagg parameter is used without specifying an individual port, a range of ports, or link aggregate ID, then the configured VLAN information for all UNP ports and link aggregates is displayed.
- The “Type” field indicates if the VLAN assignment is untagged (unpUntag) or tagged (unpQtag).

Examples

- show unp port configured-vlans
  Port  Vlan   Type
  -------+--------+--------
  0/10   500    unpUntag
  0/10   501    unpUntag
  1/1/10 600    unpQtag
  1/1/11 601    unpUntag
  1/1/11 602    unpQtag
  1/1/11 603    unpQtag

- show unp port 1/1/11 configured-vlans
  Port  Vlan   Type
  -------+--------+--------
  1/1/11 601    unpUntag
1/1/11    602  unpQtag
1/1/11    603  unpQtag

-> show unp linkagg configured-vlans

| LagId | Vlan | Type    |
|-------+------+---------|
| 0/10  | 500  | unpUntag|
| 0/10  | 501  | unpQtag |
| 0/100 | 100  | unpQtag |
| 0/100 | 101  | unpUntag|
| 0/101 | 200  | unpQtag |
| 0/101 | 201  | unpQtag |

-> show unp linkagg 100 configured-vlans

| LagId | Vlan | Type    |
|-------+------+---------|
| 0/100 | 100  | unpQtag |
| 0/100 | 101  | unpUntag|

**Release History**

Release 8.2.1; command was introduced.
Release 8.5R4; “Type” field added.

**Related Commands**

- **unp vlan** Configures VLAN assignments for UNP bridge ports.
- **show unp port** Displays the UNP port and link aggregate configuration for the switch.

**MIB Objects**

- `alaDaUNPPortVlanTable`
- `alaDaUNPPortVlanVID`
show unp port profile

Displays the UNP service profiles that are statically assigned to UNP ports or link aggregates.

show unp {port [chassis/slot/port1[-port2]] | linkagg [agg_id][-agg_id2]} profile

Syntax Definitions

chassis/slot/port[-port2] The chassis ID, slot, and port number (3/1/1) for a specific UNP port. Use a hyphen to specify a range of ports (3/1/1-8).

agg_id[-agg_id2] Link aggregate ID for a specific UNP link aggregate. Use a hyphen to specify a range of link aggregate IDs (10-15).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the port or linkagg parameter to display information for a specific UNP port or link aggregate ID.
- If the port or linkagg parameter is used without specifying an individual port, a range of ports, or link aggregate ID, then the static profile information for all UNP ports and link aggregates is displayed.

Examples

-> show unp port profile
Port Profile
---------------
1/1/5 static-spb1
1/1/5 static-spb2
1/1/10 static-vxlan1
1/1/10 static-vxlan2
1/1/20 static-l2gre

-> show unp port 1/1/5 profile
Port Profile
---------------
1/1/5 static-spb1
1/1/5 static-spb2
**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- **unp port profile**  
  Configures static profile assignments for UNP ports.

- **show unp port**  
  Displays the UNP port and link aggregate configuration for the switch.

**MIB Objects**

- **alaDaUNPPortTable**
  - **alaDaUNPPortProfile**
show unp port-template

Displays the port template configuration for the switch.

show unp port-template [template_name] [config | configured-vlans | profile]

Syntax Definitions

template_name
The name of the UNP port template to display.

config
Displays additional details about the parameter configuration for the template.

configured-vlans
Displays the VLAN IDs that the specified template assigns to a UNP port.

profile
Displays the names of UNP service profiles that the specified template assigns as static profiles to a UNP port.

Defaults

By default, displays a summary of the configuration information for all port templates.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Enter a template name with this command to display information for a specific port template.
- Use the config option with this command to display the full configuration for each template.
- Use the configured-vlans option with this command to display the VLAN IDs that a port template will statically assign to a UNP bridge port when the template is applied on the port. Configuring a static VLAN-port association (VPA) applies only to UNP bridge ports.
- Use the profile option with this command to display the names of UNP service profiles that a port template will assign as a static profile to a UNP port when the template is applied on the port.

Examples

-> show unp port-template

<table>
<thead>
<tr>
<th>Template Name</th>
<th>802.1x</th>
<th>Pass-Alt Profile</th>
<th>Mac-Auth</th>
<th>Pass-Alt Profile</th>
<th>Port-Bounce Class.</th>
<th>Trust-Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp-port1</td>
<td>Enabled</td>
<td>Pass-Alt Profile</td>
<td>Disabled</td>
<td>Pass-Alt Profile</td>
<td>Port-Bounce Class.</td>
<td>Trust-Tag</td>
</tr>
<tr>
<td>unp-port2</td>
<td>Disabled</td>
<td>Pass-Alt Profile</td>
<td>Disabled</td>
<td>Pass-Alt Profile</td>
<td>Port-Bounce Class.</td>
<td>Trust-Tag</td>
</tr>
<tr>
<td>accessDefaultPortTemplate</td>
<td>Enabled</td>
<td>Pass-Alt Profile</td>
<td>Disabled</td>
<td>Pass-Alt Profile</td>
<td>Port-Bounce Class.</td>
<td>Trust-Tag</td>
</tr>
<tr>
<td>bridgeDefaultPortTemplate</td>
<td>Enabled</td>
<td>Pass-Alt Profile</td>
<td>Disabled</td>
<td>Pass-Alt Profile</td>
<td>Port-Bounce Class.</td>
<td>Trust-Tag</td>
</tr>
</tbody>
</table>
Total Port-Template Count: 4

```
-> show unp port-template unp-port2

<table>
<thead>
<tr>
<th>Template Name</th>
<th>802.1x</th>
<th>Pass-Alt Profile</th>
<th>Mac-Auth</th>
<th>Pass-Alt Profile</th>
<th>Redirect</th>
<th>Trust-Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>unp-port2</td>
<td>Disabled</td>
<td>-</td>
<td>Enabled</td>
<td>macPass</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

-> show unp port-template accessDefaultPortTemplate

<table>
<thead>
<tr>
<th>Template Name</th>
<th>802.1x</th>
<th>Pass-Alt Profile</th>
<th>Mac-Auth</th>
<th>Pass-Alt Profile</th>
<th>Redirect</th>
<th>Trust-Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>accessDefaultPortTemplate</td>
<td>Enabled</td>
<td>-</td>
<td>Disabled</td>
<td>-</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

-> show unp port-template port-2 config

Port Template: unp-port2

- 802.1x Authentication = Disabled,
- 802.1x Pass Alternate Profile = -,
- Mac Authentication = Enabled,
- Mac-Auth Pass Alternate Profile = macPass,
- Classification = Enabled,
- Trust-tag = Enabled,
- Default Profile = -,
- Port Domain Num = 0,
- AAA-Profile = -,
- Redirect Port Bounce = Disabled,
- Port Control Direction = Both,
- 802.1x Tx-Period = 0,
- 802.1x Supp-Timeout = 0,
- 802.1x Max-Req = 2,
- 802.1x Bypass = Disabled,
- 802.1x failure-policy = default,
- Mac-auth allow-eap = -,
- Force L3-Learning = Disabled
- Force L3-Learning Port Bounce = Disabled
- Admin State = Enabled,
- Dynamic Service = -,
- L2 Profile = -,
- AP Mode = Enabled,

-> show unp port-template accessDefaultPortTemplate config

Port Template: accessDefaultPortTemplate

- 802.1x Authentication = Enabled,
- 802.1x Pass Alternate Profile = -,
- Mac Authentication = Enabled,
- Mac-Auth Pass Alternate Profile = -,
- Classification = Enabled,
- Trust-tag = Enabled,
- Default Profile = -,
- Port Domain Num = 0,
- Redirect Port Bounce = Disabled,
- AAA Profile = -,
- Port Control Direction = Both,
- 802.1x Tx-Period = 30,
- 802.1x Supp-Timeout = 30,
- 802.1x Max-Req = 2,
- 802.1x Bypass = Disabled,
- 802.1x failure-policy = default,
- Mac-auth allow-eap = -,
- Force L3-Learning = Disabled
Force L3-Learning Port Bounce = Enabled
Admin State = Enabled,
Dynamic Service = spb,
L2 Profile = “unp-def-access-profile”,
AP Mode = -, 

output definitions

<table>
<thead>
<tr>
<th>Port Template</th>
<th>The name of the port template. By default, the “accessDefaultPortTemplate” is assigned to UNP access ports and the “bridgeDefaultPortTemplate” is assigned to UNP bridge ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1x Authentication</td>
<td>The 802.1X authentication status (Enabled or Disabled).</td>
</tr>
<tr>
<td>802.1x Pass Alternate Profile</td>
<td>The name of an alternate profile for devices that pass 802.1X authentication.</td>
</tr>
<tr>
<td>Mac Authentication</td>
<td>The MAC authentication status (Enabled or Disabled).</td>
</tr>
<tr>
<td>Mac-Auth Pass Alternate Profile</td>
<td>The name of an alternate profile for devices that pass MAC authentication.</td>
</tr>
<tr>
<td>Classification</td>
<td>The classification status (Enabled or Disabled).</td>
</tr>
<tr>
<td>Trust-Tag</td>
<td>The trust VLAN ID tag status (Enabled or Disabled).</td>
</tr>
<tr>
<td>Default Profile</td>
<td>The name of a default profile for devices that are not classified by any other classification methods.</td>
</tr>
<tr>
<td>Port Domain Num</td>
<td>The domain ID number assignment for the UNP port.</td>
</tr>
<tr>
<td>Redirect Port Bounce</td>
<td>The status of port bounce (Enabled or Disabled) for BYOD registration and authorization. This parameter is only configurable on UNP bridge ports.</td>
</tr>
<tr>
<td>AAA Profile</td>
<td>The name of an AAA profile to apply to the port.</td>
</tr>
<tr>
<td>Port Control Direction</td>
<td>Whether 802.1X access control is applied to ingress and egress traffic (both) or just ingress traffic (in). This parameter is only configurable on UNP bridge ports.</td>
</tr>
<tr>
<td>802.1x Tx-Period</td>
<td>The amount of time, in seconds, before an EAP Request Identity is retransmitted.</td>
</tr>
<tr>
<td>802.1x Supp-Timeout</td>
<td>The amount of time, in seconds, the switch will wait before timing out an 802.1X user that is attempting to authenticate.</td>
</tr>
<tr>
<td>802.1x Max-Req</td>
<td>The maximum number of times the switch will retransmit a request for authentication information.</td>
</tr>
<tr>
<td>802.1x Bypass</td>
<td>The status of 802.1X bypass (Enabled or Disabled).</td>
</tr>
<tr>
<td>802.1x failure-policy</td>
<td>Whether the switch attempts subsequent MAC authentication for a device after the initial 802.1X authentication process fails (default = no MAC authentication is attempted or mac-authentication).</td>
</tr>
<tr>
<td>Mac-auth allow-eap</td>
<td>The conditions under which 802.1X authentication is performed or bypassed based on the initial MAC authentication process (pass = if MAC authentication passes, fail = if MAC authentication fails, or noauth = if MAC authentication is not configured). This parameter option only applies to UNP ports on which 802.1X authentication bypass is enabled.</td>
</tr>
<tr>
<td>Force L3-Learning</td>
<td>The status of Layer 3 learning (Enabled or Disabled).</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Force L3-Learning Port Bounce</th>
<th>The status of the port bounce action, which is an optional parameter associated with the Layer 3 learning function.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>The administrative status of the UNP port configuration (Enabled or Disabled).</td>
</tr>
<tr>
<td>Dynamic Service</td>
<td>Whether the UNP port generates dynamic SPB or VXLAN services. This parameter is only configurable on UNP access ports.</td>
</tr>
<tr>
<td>L2 Profile</td>
<td>The name of a Layer 2 service profile to apply to a UNP access port. This parameter is not configurable when the template is assigned to a UNP bridge port.</td>
</tr>
<tr>
<td>AP Mode</td>
<td>The status of Access Point (AP) mode functionality (Enabled or Disabled). This parameter is only configurable on UNP bridge ports.</td>
</tr>
</tbody>
</table>

```
-> show unp port-template unp-pton configured-vlans
Template Name | Vlan  | Type    |
---------------|-------|---------|
unp-pton       | 200   | unpUntag |
unp-pton       | 201   | unpQtag |
```

output definitions

<table>
<thead>
<tr>
<th>Template Name</th>
<th>The name of a UNP port template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>The VLAN IDs that are assigned to a UNP bridge port when the template is applied to the port.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates if the VLAN assignment is untagged (unpUntag) or tagged (unpQtag).</td>
</tr>
</tbody>
</table>

```
-> show unp port-template unp-port1 profile
Template Name | Profile |
---------------|---------|
unp-port1      | static-spb1 |
unp-port1      | static-spb2 |
```

output definitions

<table>
<thead>
<tr>
<th>Template Name</th>
<th>The name of a UNP port template.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>The name of UNP service profiles that are statically assigned to a UNP port when the template is applied to the port.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.3.1; command was introduced.
Release 8.3.1.R02; “Force L3-Learning” and “Force L3-Learning Port Bounce” fields added.
Release 8.4.1; “L2 Profile” field added.
Release 8.5R4; profile parameter added, “Type” field added to configured VLANs display.
Release 8.6R1; “AP Mode” field added.
Related Commands

unp port-template

Configures UNP port parameter values for a port template.

unp port port-template

Assigns a port configuration template to a UNP port.

show unp port config

Displays the full UNP configuration for a port, including the name of a port template that is associated with the port.

MIB Objects

alaDaUNPPortTemplateTable
alaDaUNPPortTemplateName
alaDaUNPPortTemplateAdminState
alaDaUNPPortTemplateDirection
alaDaUNPPortTemplateDomainID
alaDaUNPPortTemplateClassification
alaDaUNPPortTemplateTrustTag
alaDaUNPPortTemplateDynamicService
alaDaUNPPortTemplateDefaultProfile
alaDaUNPPortTemplateAAAProfile
alaDaUNPPortTemplateRedirectPortBounce
alaDaUNPPortTemplate8021XAuth
alaDaUNPPortTemplate8021XAuthPassAlternate
alaDaUNPPortTemplate8021XAuthBypass
alaDaUNPPortTemplate8021XAuthFailPolicy
alaDaUNPPortTemplate8021XAuthTxPeriod
alaDaUNPPortTemplate8021XAuthSuppTimeout
alaDaUNPPortTemplate8021XAuthMaxReq
alaDaUNPPortTemplateMACAuth
alaDaUNPPortTemplateMACAuthPassAlternate
alaDaUNPPortTemplateMACAuthAllowEAP
alaDaUNPPortTemplateForceL3Learning
alaDaUNPPortTemplateForceL3LearningPortBounce
alaDaUNPPortTemplateL2Profile
alaDaUNPPortTemplateApMode
alaDaUNPPortTemplateVlanTable
alaDaUNPPortTemplateVlanVID
alaDaUNPPortTemplateProfileTable
alaDaUNPPortTemplateProfile
**show unp user**

Displays information about the MAC addresses learned on a UNP port or link aggregate.

```
show unp user [port chassis/slot/port[1-port2] | linkagg agg_id[-agg_id2]] [sap-id sap_id] [service-id service_id] [profile profile_name] [authentication-type {none | mac | 802.1x}] [mac-address mac_address] [count]
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). This parameter displays all UNP users learned on the specified port number.
- **agg_id[-agg_id2]**: Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15). This parameter displays all UNP users learned on the specified link aggregate ID.
- **sap_id**: A Service Access Point (SAP) ID. This parameter displays all UNP users associated with the specified SAP ID.
- **service_id**: A service ID number. This parameter displays all UNP users associated with the specified service ID.
- **profile_name**: The name of an existing UNP profile. This parameter displays all UNP users associated with the specified profile name.
- **none**: Displays all UNP users that did not undergo the authentication process.
- **mac**: Displays all UNP users that were authenticated through the MAC authentication process.
- **802.1x**: Displays all UNP users that were authenticated through the 802.1X authentication process.
- **mac_address**: A source MAC address. This parameter displays the UNP user device with the specified source MAC address.
- **count**: Displays the number of UNP users learned on the switch.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the optional parameters provided with this command to filter the output display results. In addition, some parameters can be combined to further narrow the display results. For example:
  - Combine the **port** or **linkagg** parameter with the **profile** parameter option to display users learned on the port or link aggregate that are classified into the specified profile.
  - Combine the **port** or **linkagg** parameter with the **authentication-type** parameter option to display users on the port or link aggregate that were authenticated with the specified authentication type.

- The “Username” field displays the user name that was entered to authenticate an 802.1X user device or the user name that was entered to successfully authenticate a user device through the Captive Portal process. However, if a user device first undergoes 802.1X authentication and then undergoes successful Captive Portal authentication, the user name entered during the Captive Portal process is displayed in this field.

- IPv6 is supported only for users learned into a VLAN or service which has an IP interface configured.

Examples

```bash
=> show unp user count
Total users: 6

=> show unp user

<table>
<thead>
<tr>
<th>Port</th>
<th>Username</th>
<th>Mac address</th>
<th>User IP (V4/V6)</th>
<th>Vlan</th>
<th>Profile</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>00:00:00:00:00:01 00:00:00:00:00:01</td>
<td>2100::3</td>
<td>unp-1</td>
<td>Access</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/2</td>
<td>00:00:00:00:00:02 00:00:00:00:00:02</td>
<td>2100::4 11</td>
<td>unp-2</td>
<td>Bridge</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/3</td>
<td>guest_user</td>
<td>00:00:00:00:00:04</td>
<td>2100::6</td>
<td>unp-guest</td>
<td>Access</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>1/7</td>
<td>00:00:00:00:00:07 00:00:00:00:00:07</td>
<td>2100::7 11</td>
<td>unp-emp</td>
<td>Bridge</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/10</td>
<td>Employee-001</td>
<td>00:00:00:00:00:03</td>
<td>2100::8 12</td>
<td>unp-emp</td>
<td>Bridge</td>
<td>Active</td>
<td></td>
</tr>
<tr>
<td>0/12</td>
<td>00:00:00:00:00:14 00:00:00:00:00:14</td>
<td>2100::9 20</td>
<td>unp-7</td>
<td>Bridge</td>
<td>Active</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total users: 6
```

**output definitions**

- **Port**: The port or link aggregate on which the MAC address was learned. A “0” indicates the UNP port is a link aggregate (e.g., 0/10 refers to link aggregate ID 10).
- **Username**: Displays either a source MAC address or a Captive Portal user name for the learned user device.
- **MAC address**: The MAC address of the user device. This field and the **Username** field may contain the same MAC address, depending on how the user device was authenticated.
- **User IP (V4/V6)**: The IP network address of the user device (IPv4 or IPv6).
- **Vlan**: The UNP VLAN ID to which the user device was assigned. This only applies for users authenticated into VLAN profiles.
- **Profile**: The name of the UNP profile to which the user device was assigned.
**output definitions**

<table>
<thead>
<tr>
<th>Type</th>
<th>The type of UNP port on which the device was learned (Bridge or Access).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the device:</td>
</tr>
<tr>
<td></td>
<td>• <strong>In progress</strong>—device learning is in progress.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Active</strong>—device is learned in forwarding state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Block</strong>—device is learned in filtering state.</td>
</tr>
</tbody>
</table>

```
-> show unp user port 1/1/3

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>Username</th>
<th>Mac address</th>
<th>IP(V4/V6)</th>
<th>Vlan</th>
<th>Profile</th>
<th>Auth</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>guest_user</td>
<td>1/1/3</td>
<td>00:00:00:00:00:04</td>
<td>2100::3</td>
<td></td>
<td></td>
<td>unp-guest</td>
<td>8021X</td>
<td>Guest</td>
</tr>
</tbody>
</table>

Total users : 1
```

```
-> show unp user linkagg 10

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>Username</th>
<th>Mac address</th>
<th>IP(V4/V6)</th>
<th>Vlan</th>
<th>Profile</th>
<th>Auth</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee-001</td>
<td>0/10</td>
<td>00:00:00:00:00:03</td>
<td>2100::2</td>
<td></td>
<td>12</td>
<td>unp-emp</td>
<td>8021X</td>
<td>Employee</td>
</tr>
</tbody>
</table>

Total users : 1
```

```
-> show unp user profile unp-emp

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>Username</th>
<th>Mac address</th>
<th>IP(V4/V6)</th>
<th>Vlan</th>
<th>Profile</th>
<th>Auth</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/7</td>
<td>1/1/7</td>
<td>00:00:00:00:00:07</td>
<td>2100::3</td>
<td></td>
<td>11</td>
<td>unp-emp</td>
<td>MAC</td>
<td>Employee</td>
</tr>
<tr>
<td>0/10</td>
<td>0/10</td>
<td>00:00:00:00:00:03</td>
<td>2100::2</td>
<td></td>
<td>12</td>
<td>unp-emp</td>
<td>8021X</td>
<td>Employee</td>
</tr>
</tbody>
</table>

Total users : 2
```

```
-> show unp user authentication-type mac

<table>
<thead>
<tr>
<th>User</th>
<th>Port</th>
<th>Username</th>
<th>Mac address</th>
<th>IP(V4/V6)</th>
<th>Vlan</th>
<th>Profile</th>
<th>Auth</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/7</td>
<td>1/1/7</td>
<td>00:00:00:00:00:07</td>
<td>2100::3</td>
<td></td>
<td>11</td>
<td>unp-emp</td>
<td>MAC</td>
<td>Employee</td>
</tr>
<tr>
<td>0/12</td>
<td>0/12</td>
<td>00:00:00:00:00:14</td>
<td>2100::2</td>
<td></td>
<td>20</td>
<td>unp-7</td>
<td>MAC</td>
<td>Employee</td>
</tr>
</tbody>
</table>

Total users : 2
```

**output definitions**

<table>
<thead>
<tr>
<th>Port</th>
<th>The port or link aggregate on which the MAC address was learned. A “0” indicates the UNP port is a link aggregate (e.g., 0/10 refers to link aggregate ID 10).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Displays either a source MAC address or a Captive Portal user name for the learned user device.</td>
</tr>
<tr>
<td>MAC address</td>
<td>The MAC address of the user device. This field and the <strong>Username</strong> field may contain the same MAC address, depending on how the user device was authenticated.</td>
</tr>
<tr>
<td>User IP (V4/V6)</td>
<td>The IP network address of the user device, IPv4 or IPv6.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The UNP VLAN ID to which the user device was assigned. This only applies for users authenticated into VLAN profiles.</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>The name of the UNP profile to which the user device was assigned.</td>
</tr>
<tr>
<td>Auth</td>
<td>The type of authentication applied to the user (none, mac, or 802.1X).</td>
</tr>
<tr>
<td>Role</td>
<td>The user role (QoS policy list) applied to the user device.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.1.1; command was introduced.
Release 8.7R1; Support for IPv6 addresses of UNP users added; “User IP” field changed to “User IP (IPv4/IPv6).

**Related Commands**

- **show unp user status**  
  Displays information about the authentication and validation status of users learned on UNP ports.

- **show unp user details**  
  Displays detailed information about user devices learned on UNP ports.

- **unp user flush**  
  Performs a MAC address flush of Access Guardian users (devices learned on UNP ports).

- **show zeroconf server policy-instances**  
  Displays the UNP configuration for the switch.

- **show unp port**  
  Displays the UNP configuration for the port.

**MIB Objects**

- **N/A**
**show unp user status**

Displays the status of the authentication and validation process for MAC addresses learned on a UNP port or link aggregate.

```
show unp user status [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2] [sap-id sap_id] [service-id service_id] [profile profile_name] [authentication-type {none | mac | 802.1x}] [mac-address mac_address]
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: Link aggregate ID. Use a hyphen to specify a range of link aggregate IDs (10-15).
- **sap_id**: A Service Access Point (SAP) ID. This parameter displays all UNP users associated with the specified SAP ID.
- **service_id**: A service ID number. This parameter displays all UNP users associated with the specified service ID.
- **profile_name**: The name of an existing UNP profile.
- **none**: Displays users that did not undergo the authentication process.
- **mac**: Displays users that were authenticated through MAC authentication.
- **802.1x**: Displays users that were authenticated through 802.1X authentication.
- **mac_address**: The user device MAC address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the optional parameters provided with this command to filter the output display results. In addition, some parameters can be combined to further narrow the display results. For example:

- Combine the `port` or `linkagg` parameter with the `profile` parameter option to display users learned on the port or link aggregate that are classified into the specified profile.
• Combine the **port** or **linkagg** parameter with the **authentication-type** parameter option to display users on the port or link aggregate that were authenticated with the specified authentication type.

**Examples**

```
-> show unp user status port 1/1/1
Profile          Profile Authentication Role  Role                 Restricted
Port  Mac address       Name     Source  Type   Status  Name  Source  CP  Redirect Access
-----+-----------------+--------+-------+------+-------+-----+-------+---+--------+-------
1/1/1 00:00:00:00:00:05 Prf1     Radius  8021x  Passed  emp1  Profile  Y  -        -
Total users : 1
```

```
-> show unp user status linkagg 100
Profile          Profile Authentication Role  Role                 Restricted
Port  Mac address       Name     Source  Type   Status  Name  Source  CP  Redirect Access
-----+-----------------+--------+-------+------+-------+-----+-------+---+--------+-------
0/100 00:00:00:00:00:06 Prf3     Radius  8021x  Passed  emp1  Profile  Y  -        -
Total users : 1
```

```
-> show unp user status authentication type MAC
Profile          Profile Authentication Role  Role                 Restricted
Port  Mac address       Name     Source  Type   Status  Name  Source  CP  Redirect Access
-----+-----------------+--------+-------+------+-------+-----+-------+---+--------+-------
1/1/2 00:00:00:00:00:15 Prf2     Alt     MAC    Passed  emp2  Profile  Y  -        -
Total users : 1
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td>The port or link aggregate on which the MAC address was learned. A “0” indicates the UNP port is a link aggregate (e.g., 0/10 refers to link aggregate ID 10).</td>
</tr>
<tr>
<td><strong>MAC address</strong></td>
<td>The MAC address of the user device.</td>
</tr>
<tr>
<td><strong>Profile Name</strong></td>
<td>The name of the UNP to which the user device was assigned.</td>
</tr>
<tr>
<td><strong>Profile Source</strong></td>
<td>The source of the profile assignment (e.g., Radius, Alt).</td>
</tr>
<tr>
<td><strong>Authentication Type</strong></td>
<td>The type of authentication applied to the user (<strong>none</strong>, <strong>mac</strong>, or <strong>802.1X</strong>).</td>
</tr>
<tr>
<td><strong>Authentication Status</strong></td>
<td>The authentication status for the device.</td>
</tr>
<tr>
<td><strong>Role Name</strong></td>
<td>The name of the user role applied to the user device.</td>
</tr>
<tr>
<td><strong>Role Source</strong></td>
<td>The source of the user role applied to the user device.</td>
</tr>
<tr>
<td><strong>CP</strong></td>
<td>Indicates if the device was authenticated through Captive Portal.</td>
</tr>
<tr>
<td><strong>Redirect</strong></td>
<td>The redirection status.</td>
</tr>
<tr>
<td><strong>Restricted Access</strong></td>
<td>Whether or not access is restricted for the user.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.1.1; command was introduced.
Related Commands

- **show unp user**
  Displays information about users learned on a UNP ports.

- **show unp user details**
  Displays detailed information about users learned on a UNP ports.

- **show zeroconf server policy-instances**
  Displays the UNP configuration for the switch.

- **show unp port**
  Displays the UNP configuration for the port.

MIB Objects

- N/A
**show unp user details**

Displays additional details about the MAC addresses learned on a UNP port or link aggregate.

```
show unp user details [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] [sap-id sap_id] [service-id service_id] [profile profile_name] [authentication-type {none | mac | 802.1x}] [mac-address mac_address]
```

### Syntax Definitions

- **chassis**
  The chassis identifier.

- **slot/port[-port2]**
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). This parameter displays all UNP users learned on the specified port number.

- **agg_id[-agg_id2]**
  Link aggregate ID number. Use a hyphen to specify a range of link aggregate IDs (10-15). This parameter displays all UNP users learned on the specified link aggregate ID.

- **sap_id**
  A Service Access Point (SAP) ID. This parameter displays all UNP users associated with the specified SAP ID.

- **service_id**
  A service ID number. This parameter displays all UNP users associated with the specified service ID.

- **profile_name**
  The name of an existing UNP profile. This parameter displays all UNP users associated with the specified profile name.

- **none**
  Displays all UNP users that did not undergo the authentication process.

- **mac**
  Displays all UNP users that were authenticated through the MAC authentication process.

- **802.1x**
  Displays all UNP users that were authenticated through the 802.1X authentication process.

- **mac_address**
  A source MAC address. This parameter displays the UNP user device with the specified source MAC address.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the optional parameters provided with this command to filter the output display results. In addition, some parameters can be combined to further narrow the display results. For example:
  - Combine the `port` or `linkagg` parameter with the `profile` parameter option to display users learned on the port or link aggregate that are classified into the specified profile.
  - Combine the `port` or `linkagg` parameter with the `authentication-type` parameter option to display users on the port or link aggregate that were authenticated with the specified authentication type.

- The “User Name” field displays the user name that was entered to authenticate an 802.1X user device or the user name that was entered to successfully authenticate a user device through the Captive Portal process. However, if a user device first undergoes 802.1X authentication and then undergoes successful Captive Portal authentication, the user name entered during the Captive Portal process is displayed in this field.

Examples

```
-> show unp user details port 1/1/10
Port:  1/1/10
    MAC-Address:  00:00:00:00:00:01
    Sap                      : -,
    Service ID               : -,
    VNID                     : -,
    VPNID                    : 200,
    ISID                     : -,
    Access Timestamp         : 04/01/1970 18:45:26,
    User Name                : guest1,
    IP-address (IPv4/IPv6)   : 10.0.0.1,
    Vlan                     : 10,
    Authentication Type      : 802.1X,
    Authentication Status    : Authenticated,
    Authentication Failure Reason : -,
    Authentication Retry Count: -,
    Authentication Server IP Used = 10.135.62.129,
    Authentication Server Used = rad1,
    Server Reply-Message     = -,  
    Profile                  : Employee,
    Profile Source           : RADIUS Server Profile,
    Profile From Auth Server : Employee,
    Session Timeout          = 43200,
    Classification profile rule : -,
    Role                     : Employee,
    Role Source              : Profile,
    User role rule           : -,
    Restricted Access        : No,
    Location Policy Status   : Passed,
    Time Policy Status       : Passed,
    Captive-Portal Status    : -,
    QMR Status               : Passed,
    Redirect Url             : -, 
    SIP Call Type            = Not in a call,
    SIP Media Type           = None,
    Applications             = None

    MAC-Address:  00:00:00:00:00:02
    Sap                      : -,
    Service ID               : -,
```
VNID                        : -,  
VPNID                       : 200,  
ISID                        : -,  
Access Timestamp            : 06/01/1989 20:45:26,  
User Name                   : guest2,  
IP-address (IPv4/IPv6)      : 20.0.0.1,  
Vlan                        : 20,  
Authentication Type         : MAC,  
Authentication Status       : Authenticated,  
Authentication Failure Reason : -,  
Authentication Retry Count  : -,  
Authentication Server IP Used   : 10.135.62.129,  
Authentication Server Used  : rad1,  
Server Reply-Message        : -,  
Profile                      : Contractor,  
Profile Source              : RADIUS Server Profile,  
Profile From Auth Server    : Contractor,  
Session Timeout             : 43200,  
Classification profile rule : -,  
Role                         : Contractor,  
Role Source                  : Profile,  
User role rule              : -,  
Restricted Access            : No,  
Location Policy Status      : Passed,  
Time Policy Status          : Passed,  
Captive-Portal Status       : Passed,  
QMR Status                   : -,  
Redirect Url                 : -,  
SIP Call Type                : Normal Call,  
SIP Media Type               : Video,  
Applications                 : None  

-> show unp user details linkagg 100  
Port: 0/100  
MAC-Address: 00:00:00:00:00:03  
Sap                          : -,  
Service ID                   : -,  
VNID                         : -,  
VPNID                        : 200,  
ISID                         : -,  
Access Timestamp             : 02/01/2013 20:45:26,  
User Name                    : guest3,  
IP-address (IPv4/IPv6)       : 30.0.0.1,  
Vlan                         : 30,  
Authentication Type          : MAC,  
Authentication Status        : Authenticated,  
Authentication Failure Reason : -,  
Authentication Retry Count   : -,  
Authentication Server IP Used   : 10.135.62.129,  
Authentication Server Used   : rad1,  
Server Reply-Message         : -,  
Profile                      : Contractor,  
Profile Source               : Auth - Pass - Default UNP,  
Profile From Auth Server     : Employee [Not Configured],  
Session Timeout              : 43200,  
Classification profile rule  : -,  
Role                         : Contractor,  
Role Source                  : Profile,  
User role rule               : -,
Restricted Access: No,
Location Policy Status: Passed,
Time Policy Status: Passed,
Captive-Portal Status: Passed,
QMR Status: -,
Redirect Url: -,
SIP Call Type: Not in a call,
SIP Media Type: None,
Applications: Facebook; rediff;

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The UNP port or link aggregate on which the device was learned.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac-address</td>
<td>The MAC address of the device.</td>
</tr>
<tr>
<td>SAP</td>
<td>The port or link aggregate and encapsulation value for an SPB or VXLAN Service Access Point (SAP).</td>
</tr>
<tr>
<td>Service ID</td>
<td>The SPB or VXLAN service ID number.</td>
</tr>
<tr>
<td>VNID</td>
<td>The VXLAN Network Identifier. This value is associated with a VXLAN service ID.</td>
</tr>
<tr>
<td>ISID</td>
<td>The SPB service instance identifier. This value is associated with an SPB service ID.</td>
</tr>
<tr>
<td>VPNID</td>
<td>The L2 GRE tunnel VPN ID.</td>
</tr>
<tr>
<td>Access Timestamp</td>
<td>The date and time the device was learned.</td>
</tr>
<tr>
<td>User Name</td>
<td>The MAC address of the user.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The VLAN ID number for the VLAN in which the device was learned.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>The type of authentication used (Mac-Authentication or 802.1x-Authentication).</td>
</tr>
<tr>
<td>Authentication Status</td>
<td>The status of the authentication process (blank “-”, Authenticated, Failed, or In Progress).</td>
</tr>
<tr>
<td>Authentication Failure Reason</td>
<td>The reason authentication failed.</td>
</tr>
<tr>
<td>Authentication Retry Count</td>
<td>The number of times authentication has been attempted.</td>
</tr>
<tr>
<td>Authentication Server IP Used</td>
<td>The IP address of the authentication server.</td>
</tr>
<tr>
<td>Authentication Server Used</td>
<td>The name of the authentication server used.</td>
</tr>
<tr>
<td>Server Reply-Message</td>
<td>Reply message from the authentication server.</td>
</tr>
<tr>
<td>Profile</td>
<td>The name of the UNP profile to which the user was assigned.</td>
</tr>
<tr>
<td>Profile Source</td>
<td>The source of the profile (returned from the server or assigned through the UNP process on the switch).</td>
</tr>
<tr>
<td>Profile From Auth Server</td>
<td>The name of the UNP profile returned from the authentication server.</td>
</tr>
<tr>
<td>Classification profile rule</td>
<td>The rule that resulted in the device classification into the UNP profile.</td>
</tr>
<tr>
<td>QMR Status</td>
<td>The Quarantine Manager Remediation status for the device.</td>
</tr>
<tr>
<td>Redirect Url</td>
<td>The URL to which the device is redirected upon classification.</td>
</tr>
<tr>
<td>SIP Call Type</td>
<td>The Session Initiation Protocol (SIP) call type status for a non-supplicant (non-802.1X) device.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>SIP Media Type</th>
<th>The SIP media type status for a non-suppliant device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>The applications a non-suppliant device is running.</td>
</tr>
</tbody>
</table>

Release History

Release 8.1.1; command was introduced.
Release 8.4.1.R02; **VPNID** field added.
Release 8.7R1; Support for IPv6 addresses of UNP users added; “IP-Address” field changed to “IP-Address (IPv4/IPv6)”.

Related Commands

- **show unp user status**: Displays information about the authentication and validation status of users learned on UNP ports.
- **unp user flush**: Performs a MAC address flush of Access Guardian users (devices learned on UNP ports).
- **show zeroconf server policy-instances**: Displays the UNP configuration for the switch.
- **show unp port**: Displays the UNP configuration for the port.

MIB Objects

N/A
show unp policy validity-period

Displays the UNP period policy configuration for the switch. This type of policy is assigned to a UNP profile and applied to devices classified into the profile.

show unp policy validity-period [policy_name]

---

Syntax Definitions

policy_name  The name of an existing UNP period policy.

---

Defaults

By default, all UNP period policies are displayed.

---

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

Usage Guidelines

Enter a UNP period policy name to display information about a specific policy.

---

Examples

-> show unp policy validity-period
Policy Days Months Hours Interval                  TZ Active
-----------------------------------------------+---------
tp1   SMTWTFS JFMAMJJASOND 08:00 - 17:00      - - -     - NO
tp2   ------- ------------ - - -     01/01/13 00:00 - 01/02/13 00:00 CST NO

Total Period Policy Count: 2

-> show unp policy validity-period tp1
Policy Days Months Hours Interval                  TZ Active
-----------------------------------------------+---------
tp1   SMTWTFS JFMAMJJASOND 08:00 - 17:00      - - -     - NO

---

Release History

Release 8.1.1; command introduced.
Related Commands

unp policy validity-period Configures a UNP period policy.
unp profile period-policy Assigns a UNP period policy to a UNP profile.

MIB Objects

alaDaUNPValidityPeriodTable
    alaDaUNPValidityPeriodTableName
    alaDaUNPValidityPeriodDays
    alaDaUNPValidityPeriodDaysStatus
    alaDaUNPValidityPeriodMonths
    alaDaUNPValidityPeriodMonthsStatus
    alaDaUNPValidityPeriodHour
    alaDaUNPValidityPeriodHourStatus
    alaDaUNPValidityPeriodEndHour
    alaDaUNPValidityPeriodInterval
    alaDaUNPValidityPeriodIntervalStatus
    alaDaUNPValidityPeriodEndInterval
    alaDaUNPValidityPeriodTimezone
    alaDaUNPValidityPeriodTimezoneStatus
    alaDaUNPValidityPeriodActiveStatus
show unp policy validity-location

Displays the UNP location policy configuration for the switch. This type of policy is assigned to a UNP profile and applied to devices classified into the profile.

show unp policy validity-location [policy_name]

Syntax Definitions

policy_name

The name of an existing UNP location policy.

Defaults

By default, all UNP location policies are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enter a location policy name to display information about a specific policy.

Examples

-> show unp policy validity location
Policy: l1
   Port            = 1/1
   System Name     = shasta
   System Location = Bangalore

Total Location Policy Count: 1

Release History

Release 8.1.1; command introduced.
Related Commands

unp policy validity-location  Configures a UNP location policy.
unp profile location-policy  Assigns a UNP location policy to a UNP profile.

MIB Objects

alaDaUNPLocationPolicyTable
  alaDaUNPLocationPolicyName
  alaDaUNPLocationPolicyPort
  alaDaUNPLocationPolicyPortHigh
  alaDaUNPLocationPolicyPortStatus
  alaDaUNPLocationPolicySystemName
  alaDaUNPLocationPolicySystemLocation
**device-profile admin-state**

Enables or disables the Device Profiling configuration on the switch.

```
device-profile admin-state {enable | disable}
```

**Syntax Definitions**

- **enable** Enables Device Profiling configuration on the switch.
- **disable** Disables Device Profiling configuration on the switch.

**Defaults**

By default Device Profiling configuration is disabled globally on the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When Device Profiling is globally enabled for the switch, Device Profiling functionality is automatically enabled on all ports and link aggregates.

**Example**

```
-> device-profile admin-state enable
-> device-profile admin-state disable
```

**Release History**

Release 8.5R2; command was introduced.

**Related Commands**

- **device-profile port linkagg** Enables or disables the Device Profiling on the ports or linkagg interface.
- **show device-profile config** Displays the global configuration of the Device Profile.

**MIB Objects**

```
alaDpAdminState
```

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 40-405
device-profile port linkagg

Enables or disables the Device Profiling on the ports or linkagg interface.

device-profile [port chassis/slot/port1[-port2] | linkagg agg_id1[-agg_id2] admin-state {enable | disable}]

Syntax Definitions

chassis The chassis identifier.
slot/port1[-port2] The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
agg_id1[-agg_id2] The link aggregate ID number. Use a hyphen to specify a range of link aggregate ID numbers (5-10).
enable Enables the Device Profiling on the specified port or linkagg.
disable Disables the Device Profiling on the specified port or linkagg.

Defaults

By default Device Profiling is enabled on all ports or linkagg when the Device Profiling feature is enabled globally on the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
| Usage Guidelines

- Use this command to disable Device Profiling on specific ports or linkagg when the Device Profiling is globally enabled on the switch.
- Device Profiling configuration is not allowed on VFL or HiGig ports.

Example

- device-profile linkagg 1 admin-state enable
- device-profile port 2/1/2-5 admin-state enable
- device-profile port 1/1/2 admin-state enable
- device-profile port 1/1/2 admin-state disable
- device-profile linkagg 1-5 admin-state disable

Release History

Release 8.5R2; command was introduced.
**Related Commands**

- `show device-profile config` Displays the global configuration of the Device Profile.
- `show device-profile catalog` Displays the details of known and unknown devices identified in the network.

**MIB Objects**

- `alaDpIfTable`
- `alaDpIfAdminStatus`
**device-profile device-type**

Adds or removes a new device type and category in the Device Profile.

```
device-profile device-type type_name device-name device_name from {mac-address mac_address | dhcp-option-55 dhcp_option}
```

```
no device-profile device-type type_name
```

### Syntax Definitions

- **type_name**: The type of the device. The device type name can be of maximum size 32 alphanumeric characters.
- **device_name**: The name of the device type. The device name can be of maximum size 32 alphanumeric characters.
- **mac_address**: The MAC address of the device. The device with that MAC address must be in the unknown cataloged devices.
- **dhcp_option**: The DHCP option 55 codes of the device.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The unknown cataloged devices can be identified or moved to trusted identity in the Device Profile using this command.
- While specifying the MAC address of the device for identity, the device must first be present in the unknown cataloged devices. Otherwise, the MAC address will not be recognized.
- Custom signatures can be created using the DHCP option 55.
- The new signatures created will not be persistent unless it is saved. Use the **device-profile update-signature** CLI command to update the flash or signature database.
- Use the **no** form of the command to remove the device and its category from the trusted device list.
Example

```plaintext
-> device-profile device-type Printer-Fax device-name Kyocera-Printer mac-address 00:aa:bb:12:43:55
-> device-profile device-type IP-Camera device-name netgear dhcp-option-55 1,3,6,15,119,252
-> no device-profile device-type Printer-Fax
```

Release History

Release 8.5R2; command was introduced.

Related Commands

- **device-profile auto-unassignment**: Enables auto assignment of UNP profile when the device gets identified and categorized into existing device types.
- **show device-profile catalog**: Displays the details of known and unknown devices identified in the network.
- **device-profile update-signature**
  - **device-profile update-signature from**: Updates the custom or user-defined device type to the flash and signature database.
  - **device-profile update-signature from**: Apply the new signature file in the system.

MIB Objects

- `alaDpDeviceTable`
  - `alaDpDeviceType`
  - `alaDpDeviceName`
  - `alaDpDeviceMacAddress`
  - `alaDpDeviceDhcpOpt55`
  - `alaDpDeviceRowStatus`
device-profile update-signature

Updates the custom or user-defined device type to the flash and signature database.

device-profile update-signature

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the flash or the signature database is not updated with the new device type, it will not be persistent.

Example

-> device-profile update-signature

Release History

Release 8.5R2; command was introduced.

Related Commands

- **show device-profile catalog**: Displays the details of known and unknown devices identified in the network.
- **device-profile update-signature from**: Apply the new signature file in the system.
- **show device-profile signatures**: Displays the device types in the local database and indicates the signatures which are not saved to the flash.

MIB Objects

alaDpUpdateSignature
alaDpUpdateSignature
device-profile update-signature from

Applies the new signature file in the system.

device-profile update-signature from file-name

Syntax Definitions

file_name The name of the file which contains device signatures.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

|    | 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900 V72/C32 | 6900 X48C6/T48C6/ | 9900 |
|----|------|------|------|-------|------|-------|------|------|--------------|X48C4E/V48C8/ |      |
|    | Yes  | Yes  | Yes  | Yes   | Yes  | Yes   | Yes  | Yes  | Yes          |C32E/T24C2/     | Yes |
|    |      |      |      |       |      |       |      |      |              |X24C2           |     |

Usage Guidelines

- Use this command to update the signature file in the system. Currently, only DHCP option 55 based signature is updated.
- The command also updates the custom signature into the flash.

Example

-> device-profile update-signature from /flash/dhcp_option55_list.txt

Release History

Release 8.5R2; command was introduced.

Related Commands

show device-profile catalog Displays the details of known and unknown devices identified in the network.

show device-profile signatures Displays the device types in the local database and indicates the signatures which are not saved to the flash.

show device-profile signatures from Displays the contents of the signature file.
**MIB Objects**

alaDpGlobalConfig

alaDpUpdateSignatureFileName
**device-profile auto-unp-assignment**

Configures the status of automatic assignment to a UNP profile when the device gets identified and categorized into existing device types.

- `device-profile auto-unp-assignment`
- `no device-profile auto-unp-assignment`

---

**Syntax Definitions**

N/A

**Defaults**

By default, automatic assignment to a UNP profile is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the device profile is from a different VLAN, then it must be port bounced using the `unp redirect port-bounce` command to toggle.
- Use the `no` form of the command to disable the auto assignment of the UNP profile.
- When Device Profiling is globally enabled for the switch, the following UNP profiles and extended classification rules are automatically created on the switch:
  - `devProfPrinter`
  - `devProfWindows`
  - `devProfIP-Phone`
  - `devProfWireless-Router`
  - `devProfSmartPhone/PDA/Tablets`
- Automatically created UNP profiles are not mapped to a VLAN; manually configuring the VLAN assignment for the profile is still required.
- UNP profiles automatically created for the device types still require mapping the profiles to a VLAN.

**Example**

- `device-profile auto-unp-assignment`
- `no device-profile auto-unp-assignment`
**Release History**

Release 8.5R2; command was introduced.

**Related Commands**

- **device-profile device-type**
  Adds or removes new device type and category in Device Profile.

- **show unp user**
  Displays information about the MAC addresses learned on a UNP port or link aggregate.

- **show unp profile**
  Displays the UNP profile configuration for the switch.

- **show unp classification-rule**
  Displays the UNP extended classification rule configuration for the switch.

- **show device-profile summary**
  Displays the number of devices identified based on the device type.

**MIB Objects**

- alaDpGlobalConfig
  - alaDpAutoUnpAssignment
show device-profile config

Displays the global configuration for Device Profiling.

show device-profile config

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X48C6/T48C6/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The command displays the non-default status per physical port and linkagg.
- The UNP profile auto-assignment status is also displayed.

**Examples**

`-> show device-profile config`

Admin-State: Enable
UNP Auto-Assignment: Disable
Interface Admin-Status
-------------+
1/1/1 Disable
1/1/2 Disable
1/1/4 Disable
0/1 Disable

**output definitions**

<table>
<thead>
<tr>
<th></th>
<th>Displays the administrative status of Device Profiling.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin-State</td>
<td>Displays the status of automatic UNP profile assignment for the identified devices.</td>
</tr>
<tr>
<td>UNP Auto-Assignment</td>
<td>Displays the interface on which Device Profiling is configured.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the administrative status of Device Profiling on the interface.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.5R2; command was introduced.

**Related Commands**

- `device-profile admin-state` Enables or disables the Device Profiling configuration on the switch.
- `device-profile port linkagg` Enables or disables Device Profiling on the ports or linkagg interface.

**MIB Objects**

- `alaDpGlobalConfig`
  - `alaDpAdminState`
  - `alaDpAutoUnpAssignment`
  - `alaDpDeviceRowStatus`
show device-profile summary

Displays the number of devices identified based on the device type. Also displays information about the number of devices identified in the last one hour and one day.

show device-profile summary

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Guardian Commands show device-profile summary</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show device-profile summary

<table>
<thead>
<tr>
<th>Device-Type</th>
<th>Total Count</th>
<th>1 Hr Count</th>
<th>1 Day Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone/PDA/Tablets</td>
<td>10</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Windows</td>
<td>5</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>IP-Camera</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>IP-Phone</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Access-Points</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Printers</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Device-Type</th>
<th>Displays the name of the device type.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Count</td>
<td>Displays the total number of devices identified for the device type.</td>
</tr>
<tr>
<td>1 Hr Count</td>
<td>Displays the number of devices identified in the last one hour for the device type.</td>
</tr>
<tr>
<td>1 Day Count</td>
<td>Displays the number of devices identified in the last one day for the device type.</td>
</tr>
</tbody>
</table>
Release History

Release 8.5R2; command was introduced.

Related Commands

device-profile device-type

Adds or removes new device type and category in Device Profile.

MIB Objects

alaDpDeviceType
alaDpDeviceRowStatus
show device-profile catalog

Displays the details of known and unknown devices identified in the network.

show device-profile catalog [unknown]

**Syntax Definitions**

**unknown**

Displays only the unknown devices discovered.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the option **unknown** in the CLI to display the unknown devices.

**Examples**

```
-> show device-profile catalog
Legend: * indicates 'Unknown/Un-catalogued' devices

<table>
<thead>
<tr>
<th>Port/ LAGG</th>
<th>Device Type</th>
<th>Device Name</th>
<th>MAC-Address</th>
<th>IP Address</th>
<th>TimeStamp Initial</th>
<th>TimeStamp Most-Recent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Smartphone</td>
<td>Apple</td>
<td>01:22:13:08:44:42</td>
<td>50.50.50.3</td>
<td>2018-03-10 8:30:00</td>
<td>2018-03-12 10:30:00</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Printers</td>
<td>Kyocera</td>
<td>00:21:23:0F:21:22</td>
<td>60.60.60.3</td>
<td>2018-03-10 8:30:00</td>
<td>2018-03-12 10:30:00</td>
</tr>
<tr>
<td>*1/1/3</td>
<td>-</td>
<td>-</td>
<td>11:32:54:0C:32:54</td>
<td>60.60.60.4</td>
<td>2018-03-10 10:00:00</td>
<td>2018-03-12 10:00:00</td>
</tr>
<tr>
<td>1/1/4</td>
<td>Access-Points</td>
<td>Stellar</td>
<td>14:44:56:0A:44:23</td>
<td>50.50.50.6</td>
<td>2018-03-10 8:00:00</td>
<td>2018-03-12 12:30:00</td>
</tr>
<tr>
<td>2/1/10</td>
<td>IP Camera</td>
<td>Samsung</td>
<td>05:44:23:00:45:66</td>
<td>50.50.50.3</td>
<td>2018-03-10 4:00:00</td>
<td>2018-03-12 11:30:00</td>
</tr>
</tbody>
</table>
```

**output definitions**

<table>
<thead>
<tr>
<th>Port/ LAGG</th>
<th>Displays the port number or the linkagg ID on which the device is identified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Type</td>
<td>Displays the device type identified.</td>
</tr>
<tr>
<td>Device Name</td>
<td>Displays the name of the device type.</td>
</tr>
<tr>
<td>MAC-Address</td>
<td>Displays the MAC address of the device.</td>
</tr>
<tr>
<td>IP-Address</td>
<td>Displays the IP address of the device.</td>
</tr>
<tr>
<td>TimeStamp Initial</td>
<td>Displays the time stamp when the device was first identified.</td>
</tr>
<tr>
<td>TimeStamp Most-Recent</td>
<td>Displays the time stamp when the device was recently active.</td>
</tr>
</tbody>
</table>
Access Guardian Commands

- show device-profile catalog unknown

<table>
<thead>
<tr>
<th>Port/LAGG</th>
<th>Mac-Address</th>
<th>DHCP VCI (Option 60)</th>
<th>DHCP Option 55</th>
<th>Mac-Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/15</td>
<td>34:E7:0B:03:CS:00 HAP.1-OAW-AP1220-US</td>
<td>1,3,6,12,15,28,42,43,66,67,138,212 HANNetwork</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/13</td>
<td>34:E7:0B:03:CS:11 HAP.1-OAW-AP1220-US</td>
<td>1,3,6,12,15,28,42,43,66,67,138,212 HANNetwork</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1/1/3</td>
<td>11:32:54:0A:32:54 alcatel.noe.0</td>
<td>1,3,28,43,58,59</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0/1</td>
<td>16:56:34:0B:33:21 -</td>
<td>1,3,6,15,119,252</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

- **Port/ LAGG**: Displays the port number or the linkagg ID on which the device is identified.
- **MAC-Address**: Displays the MAC address of the device.
- **DHCP VCI (Option 60)**: Displays the DHCP option 60 information of the device.
- **DHCP Option 55**: Displays the DHCP option 55 information of the device.
- **Mac-Vendor**: Displays the unique MAC identifier for the vendor.

**Release History**

Release 8.5R2; command was introduced.
Release 8.6R1; “IP Address” field added.

**Related Commands**

- **device-profile port linkagg**: Enables or disables the Device Profiling on the ports or linkagg interface.

**MIB Objects**

alaDpDeviceTable
  - alaDpDeviceType
  - alaDpDeviceName
  - alaDpDeviceMacAddress
show device-profile signatures from

Displays the contents of the signature file.

show device-profile signatures from file-name

Syntax Definitions

file_name : The name of the file which contains device signatures.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show device-profile signatures from device_profile_sigs.csv

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Device Name</th>
<th>DHCP Option 55</th>
</tr>
</thead>
<tbody>
<tr>
<td>ale-ip-phone</td>
<td>ale-ip-phone</td>
<td>1,3,6,12,15,28,42,43,66,67,138,212</td>
</tr>
<tr>
<td>IP-Phone</td>
<td>IP-Phone</td>
<td>1,3,6,12,15,28,42,43,60,61,66</td>
</tr>
<tr>
<td>AP</td>
<td>AP</td>
<td>1,3,6,12,15,28,42,43,66,67,138,212</td>
</tr>
<tr>
<td>Smartphone/PDA</td>
<td>Smartphone</td>
<td>1,3,3,6,15,28,51,58,59</td>
</tr>
<tr>
<td>PDA/Tablets</td>
<td>PDA</td>
<td>1,3,3,6,15,28,51,58,59,43</td>
</tr>
<tr>
<td>AP</td>
<td>AP</td>
<td>1,3,6,12,15,28,42,43,66,67,138</td>
</tr>
<tr>
<td>PDA/Tablets</td>
<td>Tablets</td>
<td>1,3,6,15,26,28,51,58,59,43</td>
</tr>
</tbody>
</table>

Number of Signatures: 7

Output definitions

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Displays the type of device identified.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Displays the name of the identified device.</td>
</tr>
<tr>
<td>DHCP Option 55</td>
<td>Displays the DHCP Option 55 information of the identified device.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.5R2; command was introduced.

**Related Commands**

`device-profile update-signature`  Applies the new signature file in the system.

**MIB Objects**

- `alaDpUpdateSignature`  
- `alaDpUpdateSignatureFileName`
show device-profile signatures

Displays the device types in the local database and indicates the signatures which are not saved to the flash.

show device-profile signatures

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Device Name</th>
<th>DHCP Option 55</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless-Router</td>
<td>D-Link DI-624+</td>
<td>1,3,6,15</td>
</tr>
<tr>
<td>Smartphone/PDA/Tablets</td>
<td>Apple iPad</td>
<td>1,3,6,15,119,252</td>
</tr>
<tr>
<td>IP-Phone</td>
<td>Gigaset A580 VoIP</td>
<td>1,3,6,120,125,114</td>
</tr>
<tr>
<td>Printer</td>
<td>Kyocera Network Printer</td>
<td>1,3,12,23,6,15,44,47</td>
</tr>
<tr>
<td>Smartphone/PDA/Tablets</td>
<td>Motorola</td>
<td>1,121,33,3,6,28,51,58,59</td>
</tr>
<tr>
<td>Windows</td>
<td>Windows XP</td>
<td>1,15,3,6,44,46,47,31,33,249,43</td>
</tr>
<tr>
<td>Windows_XP</td>
<td>MY_PC</td>
<td>1,15,3,6,44,46,47,31,33,121,249,43</td>
</tr>
<tr>
<td>WIN</td>
<td>new_pc</td>
<td>1,15,3,6,44,46,47,31,33,121,249,252,43</td>
</tr>
<tr>
<td>NEW_WIN</td>
<td>this_pc</td>
<td>1,15,3,6,44,46,47,31,33,121,249,43,252</td>
</tr>
<tr>
<td>Printer</td>
<td>SAMSUNG Network</td>
<td>1,3,6,7,12,15,18,23,26,44,46,51,54,58,59,78,79,81</td>
</tr>
<tr>
<td>*new</td>
<td>new_name</td>
<td>1,3,12,23,6,58,249</td>
</tr>
</tbody>
</table>

Number of Signatures: 13

Usage Guidelines

- Displays all the device types in the local database (/flash file).
- An asterisk (*) next to the device type indicates that the device signature is not saved to the flash.

Examples

-> show device-profile signatures
**output definitions**

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Displays the device type of the signature. An asterisk (*) indicates the signature of the device is not saved to the flash.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Displays the device name associated with the device type.</td>
</tr>
<tr>
<td>DHCP Option 55</td>
<td>Displays the DHCP option 55 parameters associated with the device.</td>
</tr>
<tr>
<td>Number of Signatures</td>
<td>Displays the total number of signatures on the switch.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R2; command was introduced.

**Related Commands**

device-profile update-signature Updates the custom or user-defined device type to the flash and signature database.

**MIB Objects**

alaDpUpdateSignature
41 Application Monitoring and Enforcement Commands

Application usage patterns in the enterprise network is changing with the increase in use of the social networking, browser based file sharing, and peer to peer applications. The use of these applications result in the new traffic patterns in the network that are not straightforward to distinguish. There is also an increase in consumerization of IT with multiplication of thin clients, HTTP based, and virtual desktop clients.

OmniSwitch Application Monitoring and Enforcement (AppMon) feature addresses the key challenges of real time classification of flows at application level by providing differential QoS treatment in the form of higher priority marking and security policies at application level. AppMon feature improves the quality of user experience through application aware network optimization and control.

Note.
- AppMon is supported on a virtual chassis of OmniSwitch 6860 and OmniSwitch 6860E platforms where at least one OmniSwitch 6860E is mandatory for the feature to work.
- AppMon is supported on a virtual chassis of OmniSwitch 6860N.

MIB information for the AppMon commands is as follows:

Filename: ALCATEL-IND1-APP-MON-MIB.mib
Module: alaAppMonMIB
A summary of the available commands is listed here:

```
app-mon admin-state
app-mon port admin-state
app-mon auto-group create
app-mon app-group
app-mon app-list
app-mon apply
app-mon l3-mode
app-mon l4-mode
app-mon l4port-exclude
app-mon flow-table flush
app-mon flow-table enforcement stats
app-mon aging enforcement
app-mon logging-threshold
app-mon flow-sync enforcement interval
app-mon force-flow-sync
app-mon separate-config-file
app-mon data
app-mon enforcement-mode
show app-mon config
show app-mon port
show app-mon app-pool
show app-mon app-list
show app-mon app-group
show app-mon app-record
show app-mon ipv4-flow-table
show app-mon ipv6-flow-table
show app-mon l4port-exclude
show app-mon stats
show app-mon aging enforcement
show app-mon vc-topology
clear app-mon app-list
```
app-mon admin-state

Enable or disable the Application Monitoring and Enforcement (AppMon) feature.

app-mon admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables AppMon support on the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables AppMon support on the switch.</td>
</tr>
</tbody>
</table>

Defaults

By default, AppMon is disabled on the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- AppMon cannot be enabled globally when,
  - all the mirroring sessions are used by port mirroring or monitoring features.
  - mirroring session is used by policy manager.
  - This is applicable for OmniSwitch 6860 only.
- On OmniSwitch 6860, when AppMon is enabled globally, it reserves a mirroring session in the system.
- If AppMon functionality is enabled at a port level, disabling AppMon globally overrides the functionality of all AppMon ports; however, configuration on the ports remain the same.
- AppMon is supported on a virtual chassis of OmniSwitch 6860 and OmniSwitch 6860E platforms where at least one OmniSwitch 6860E is mandatory for the feature to work.
- AppMon is supported on a virtual chassis of OmniSwitch 6860N.

Examples

- `-> app-mon admin-state enable`
- `-> app-mon admin-state disable`

Release History

Release 8.2.1; command introduced.
Related Commands

app-mon port admin-state
Enable or disable AppMon on one or more switch ports.

show app-mon config
Displays global AppMon configuration.

MIB Objects

alaAppMonAdminStatus
app-mon port admin-state

Enable or disable AppMon Monitoring and Enforcement on one or more switch ports.

```
app-mon {port chassis/slot/port[-port2] | slot chassis/slot [-slot]} admin-state {enable | disable}
```

**Syntax Definitions**

- `chassis/slot/port[-port2]`: The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
- `chassis/slot`: The chassis ID and slot number (3/1) for a specific slot.
- `enable`: Enables AppMon on the port.
- `disable`: Disables AppMon on the port.

**Defaults**

By default, AppMon is disabled on all ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- It is mandatory to enable AppMon globally for the port level AppMon to function.
- When slot option is used, then AppMon configuration is applied on all the physical ports of that particular slot.
- AppMon configuration is not allowed on Virtual Fabric Link, ERP, or VLAN stacking ports.
- On OmniSwitch 6860, AppMon cannot be configured on a port that is part of a link aggregate or a port mirroring port. On OmniSwitch 6860N, AppMon can be configured on a port that is part of a link aggregate.
- On OmniSwitch 6860, AppMon must not be configured on user ports and uplink ports at the same time. On OmniSwitch 6860N, it is mandatory to enable AppMon on user ports and uplink ports.
- On OmniSwitch 6860N, AppMon must be enabled on both ports involving bi-direction flow traffic.

**Examples**

- `-> app-mon slot 1/1 admin-state enable`
- `-> app-mon port 1/1/2-5 admin-state enable`
- `-> app-mon slot 1/1 admin-state disable`
**Release History**

Release 8.2.1; command introduced.
Release 8.7R1; AppMon support on SPB/UNP access ports added.
Release 8.8R1; AppMon support on SPB/UNP access ports added on OmniSwitch 6860N.

**Related Commands**

- **app-mon admin-state**  
  Enable or disable the Application Monitoring feature.
- **show app-mon port**  
  Displays AppMon status per physical port or per slot for the switch.

**MIB Objects**

alaAppMonPortConfigTable

- alaAppMonPortConfigSlotPortIndex
- alaAppMonPortConfigPortStatus
app-mon auto-group create

Creates application groups automatically on the switch. The application groups are automatically created based on the ‘category’ field of each application present in the application pool.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Modifications are allowed in auto application groups with addition or deletion of applications using the app-mon app-group command.

- Enter app-mon apply and write memory to save the auto group configuration or modification on the switch.

- The show app-mon app-pool command displays the application categories in the signature file. The application group names are derived from the category name.

Examples

-> app-mon auto-group create

Release History

Release 8.2.1; command introduced.
Related Commands

- **app-mon apply**  
  Updates the set of application signatures configured for application monitoring.

- **show app-mon app-group**  
  Displays the details of all the applications in an application group.

- **show app-mon app-pool**  
  Displays all the applications that are part of an application pool.

MIB Objects

- **alaAppMonAutoGroupCreation**
**app-mon app-group**

Creates an application group. Applications can be added or removed from the application group.

```
app-mon app-group app_group_name {add | remove} {app-name app_name | from app_name to app_name}
```

```
no app-mon app-group app_group_name
```

**Syntax Definitions**

- `app_group_name`: Name of the application group. The group name can be a maximum of 32 alphanumeric characters.
- `app_name`: The name of the application to be added to the application group. The application name can be a maximum of 32 alphanumeric characters.
- `from app_name`: The first application name when adding a range of applications to an application group.
- `to app_name`: The last application name when adding a range of applications to an application group.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove an application group.
- This command can be used to add or delete applications for the auto application groups as well.
- One application can belong to more than one application group.
- Only those applications that are part of an application pool are allowed to be added to an application group.
- To add a range of applications or multiple applications to an application group, use the **from** and **to** options. Range is expanded based on the list of applications in the app-pool list (application pool). Use the **show app-mon app-pool** command to view the application names.
- If an application is removed from an application group which has only one application, then the complete application group is removed.
- If any application is added to a user group (group name same name as category name), and signature toolkit update operation or 'app-mon auto-group create' is done, then added group is not deleted. Only update happens.

- If an application group contains a single application and the group is part of an application list, then this single application cannot be removed from the application group.

- An application group cannot be deleted when it is part of an application list.

- When the last application from the application group is removed, the application group is automatically deleted.

- The list of applications (added or deleted) to an application group is displayed in show configuration snapshot command after app-mon apply command is entered. A list of applications (added or deleted) are displayed with the show app-mon app-group command even without using the app-mon apply command.

**Examples**

```
-> app-mon app-group apg2 add app-name whatsapp
-> app-mon app-group apg2 remove app-name whatsapp
-> no app-mon app-group apg2
```

To add a range of applications or multiple applications to an application group, use the show app-mon app-pool command to view the application names. For example:

```
-> show app-mon app-pool
Legend: Application-name: *= Not present in recently updated kit,
AppId | Application-name | Revision | Category
-------+-----------------+----------+----------------
968 | amazon | 1.0.0 | Web
244 | facebook | 1.0.0 | Web
182 | sip | 1.0.0 | Audio/Video
183 | skype | 1.1.0 | Instant Messaging
211 | tftp | 1.0.0 | File Server
503 | twitter | 1.0.0 | Web
597 | viber | 1.0.0 | Audio/Video
890 | webex | 1.0.0 | Audio/Video
1093 | whatsapp | 1.0.0 | Instant Messaging
240 | youtube | 1.0.0 | Web
```

Number of Applications: 10

Select any two applications for the range option using the app-mon app-group command.

```
-> app-mon app-group apg1 add from sip to viber
```

This command adds the applications from sip to viber to the application group (sip, skype, tftp, twitter, and viber).

If an application is removed from an application group which has only one application, then the complete application group is removed. For example:

```
-> show app-mon app-group group1
AppGrp-Id | App-group | App-name
----------+-----------+-------------------
1093 | whatsapp | Instant Messaging
```

Now, remove the application name ‘whatsapp’ from the application group. The complete application group gets removed as shown below.
AppGrp-Id   App-group   App-name
------------+-------------------------+-------------------------

**Release History**

Release 8.2.1; command introduced.

**Related Commands**

- **app-mon apply** Updates the set of application signatures configured for application monitoring.
- **show app-mon app-group** Displays the details of all the applications in an application group.
- **show app-mon app-list** Displays a list of applications and application groups added to an application list.
- **show app-mon app-pool** Displays all the applications that are part of an application pool.

**MIB Objects**

alaAppMonAppGroupTable
  alaAppMonAppGroupName
  alaAppMonAppGroupMember
  alaAppMonAppGroupStatus
  alaAppMonAppGrpFromAppName
  alaAppMonAppGrpToAppName
  alaAppMonAddAppGrpName
  alaAppMonAppGroupBuiltIn
  alaAppMonAppGroupCategoryName
  alaAppMonAppGrpId
  alaAppMonAppGroupAppStatus
**app-mon app-list**

Add or remove applications or application groups to an application list for enforcement or monitoring.

```
app-mon app-list {enforcement | monitor} {add | remove} {app-name app_name | app-group app_group_name}
```

**Syntax Definitions**

- **add**: Adds the specified application or application group to an application list.
- **remove**: Removes the specified application or application group from an application list.
- **app_name**: Name of the application to be added to the application list. This adds the specified application to the application list.
- **app_group_name**: Name of the application group to be added to the application list. This enables the addition of multiple applications in the application group to the application list.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The application group can be user created or generated automatically (see `app-mon app-group` and `app-mon auto-group create` command).
- Separate application list is maintained for enforcement and monitoring.
- The `show configuration snapshot` command displays the applications added or removed from the application list only after the `app-mon apply` command is used. The `app-mon apply` command saves the list of applications added or removed to the application list. The saved list of applications are displayed with the `show app-mon app-list active` command.
- QoS policy rules can be configured for a given application as well as an application group where the same application also exists. QoS matches policies based on the application-name or application-group name configured in an application list. For more information on configuring enforcement for QoS policy rules, see the “QoS Policy Commands” chapter.
Examples

-> app-mon app-list enforcement add app-name whatsapp
-> app-mon app-list enforcement add app-group apg1
-> app-mon app-list monitor add app-group apg2
-> app-mon app-list enforcement remove app-name whatsapp

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon auto-group create  Enables or disables Auto-Group functionality on the switch.
app-mon app-group       Creates an application group. Applications can be added or removed from the application group.
show app-mon app-list   Displays list of applications and application groups added to an application list.
clear app-mon app-list  Removes all applications signatures from the application list.

MIB Objects

alaAppMonAppListTable
  alaAppMonAppListMemberName
  alaAppMonAppListMemberType
  alaAppMonAppListMemberStatus
  alaAppMonAppListAppId
  alaAppMonAppListAppStatus
**app-mon apply**

This activates both enforcement and monitoring application lists for flow classification.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The following operations are performed with the `app-mon apply` command:

- Saves the current application-list, application-group, and auto-groups to flash when 'write memory' command is used.

- The application list is checked for any application configured more than once in an application list (individually or as a part of application group).
  - The `app-mon apply` command will not be successful until the conflict is resolved.
  - The `show app-mon app-list` command with the `monitor conflict` or the `enforcement conflict` parameter displays the available conflicts in an application list.
  - The duplicate application names must be removed for a successful `app-mon apply` operation.

- QoS is applied to the flows learned for the activated applications based on the configured QoS policies for Enforcement application list.

**Examples**

`-> app-mon apply`

**Release History**

Release 8.2.1; command introduced.
Related Commands

- **show app-mon config**
  Displays global AppMon configuration.

- **show app-mon port**
  Displays AppMon status per physical port or per slot for the switch.

- **show app-mon app-list**
  Displays a list of applications and application groups added to an application list.

MIB Objects

`alaAppMonUpdateAppList`
**app-mon l3-mode**

Enables or disables monitoring and enforcement for IPv4 flows, IPv6 flows, or both.

```
app-mon l3-mode {ipv4 | ipv6} admin-state {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
<th>enable</th>
<th>disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applies monitoring and enforcement to IPv4 flows.</td>
<td>Applies monitoring and enforcement to IPv6 flows.</td>
<td>Enables the specified L3 mode on the switch.</td>
<td>Disables the specified L3 mode on the switch.</td>
</tr>
</tbody>
</table>

### Defaults

By default, monitoring and enforcement is enabled for both IPv4 and IPv6 flows.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> app-mon l3-mode ipv4 admin-state disable
-> app-mon l3-mode ipv4 admin-state enable
-> app-mon l3-mode ipv6 admin-state disable
```

### Release History

Release 8.2.1; command introduced.
Related Commands

**show app-mon ipv4-flow-table**  Displays the flow table for IPv4 flows entries for enforcement and monitor flows.

**show app-mon ipv6-flow-table**  Displays the flow table for IPv6 flows entries for enforcement and monitor flows.

**show app-mon config**  Displays global AppMon configuration.

MIB Objects

- `alaAppMonEnforcementIpv4`
- `alaAppMonEnforcementIpv6`
**app-mon l4-mode**

Enables or disables monitoring and enforcement for TCP or UDP flows.

```
app-mon {port chassis/slot/port[-port2] | slot chassis/slot} l4-mode {tcp | udp} admin-state {enable | disable}
```

### Syntax Definitions

- `chassis/slot/port[-port2]` The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).
- `chassis/slot` The chassis ID and slot number (3/1) for a specific slot.
- `tcp` Applies monitoring and enforcement to TCP flows.
- `udp` Applies monitoring and enforcement to UDP flows.
- `enable` Enables the specified L4 mode on the switch.
- `disable` Disables the specified L4 mode on the switch.

### Defaults

By default, both TCP and UDP flows are processed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

- `-> app-mon port 1/1/2 l4-mode udp admin-state disable`
- `-> app-mon slot 1/1 l4-mode tcp admin-state enable`
- `-> app-mon port 1/1/2 l4-mode udp admin-state enable`

### Release History

Release 8.2.1; command introduced.
**Related Commands**

- `app-mon l4port-exclude`  Configures the L4 port range to exclude from the AppMon operation.
- `show app-mon ipv4-flow-table`  Displays the flow table for IPv4 flows entries for enforcement and monitor flows.
- `show app-mon ipv6-flow-table`  Displays the flow table for IPv6 flows entries for enforcement and monitor flows.
- `show app-mon config`  Displays global AppMon configuration.

**MIB Objects**

- `alaAppMonPortConfigTable`
  - `alaAppMonPortConfigSlotPortIndex`
  - `alaAppMonEnforcementPortConfigTcpStatus`
  - `alaAppMonEnforcementPortConfigUdpStatus`
app-mon l4port-exclude

Configures the L4 port range to exclude from the AppMon operation.

app-mon l4port-exclude range-id number \{tcp-service-port | udp-port\} start number end number

no app-mon l4port-exclude range-id

Syntax Definitions

range-id number The range ID number. The valid range is 1–8.
tcp-service-port Specifies TCP service ports.
udp-port Specifies UDP ports.
start number The first port associated with the range ID number. The valid port range is 1–65535.
end number The last port associated with the range ID number. The valid port range is 1–65535.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove an L4 exclude range ID from the switch configuration.
- For the udp-port option, the AppMon operation is not performed on the flows with a source or destination port that is in the excluded port range.
- For the tcp-service-port option, the AppMon operation is not performed on the flows with a destination TCP port of TCP-SYN packet or a source TCP port of TCP-SYN-ACK packet that is in the excluded port range.
- This configuration applies to both enforcement and monitor features.

Examples

-> app-mon l4port-exclude range-id 5 tcp-service-port start 20 end 30
-> app-mon l4port-exclude range-id 6 udp-port start 90 end 100
-> no app-mon l4port-exclude range-id 6
Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon l4port-exclude Displays the port range excluded from AppMon operation.

MIB Objects

alaAppMonEnforcementL4PortRangeTable
   alaAppMonEnforcementL4PortRangeStart
   alaAppMonEnforcementL4PortRangeEnd
   alaAppMonEnforcementL4PortType
   alaAppMonEnforcementL4PortStatus
app-mon flow-table flush

Clears all the learned flow-table entries for both IPv4 and IPv6 flow tables.

app-mon flow-table {enforcement | monitor} flush

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enforcement</td>
<td>Flushes all the learned flow-table entries from the enforcement application.</td>
</tr>
<tr>
<td>monitor</td>
<td>Flushes all the learned flow-table entries from the monitor application.</td>
</tr>
</tbody>
</table>

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the *enforcement* option is used, all the active flows information are cleared; no QoS treatment is provided (if configured). The data (active, gross counters, statistics, and flow information) in the following commands are cleared: show app-mon app-list enforcement active, show app-mon app-list enforcement active stats, show app-mon ipv4-flow-table enforcement, show app-mon ipv6-flow-table enforcement, show app-mon stats.

- When the *monitor* option is used, all the learned flows information will be cleared. The data (gross counters and flow information) in the following commands are cleared: show app-mon app-list monitor active, show app-mon ipv4-flow-table monitor, show app-mon ipv6-flow-table monitor.

- When this command is used, application-record information is not cleared.

**Examples**

- `app-mon flow-table enforcement flush`
- `app-mon flow-table monitor flush`

**Release History**

Release 8.2.1; command introduced.
**Related Commands**

- `show app-mon config` Displays global AppMon configuration.
- `show app-mon app-list` Displays a list of applications and application groups added to an application list. ‘stats’ option in this command displays active or gross packets/byte counters on per application basis.
- `show app-mon ipv4-flow-table` Displays the flow table for IPv4 flows entries for enforcement and monitor flows.
- `show app-mon ipv6-flow-table` Displays the flow table for IPv6 flows entries for enforcement and monitor flows.

**MIB Objects**

- `alaAppMonFlowTableFlush`
**app-mon flow-table enforcement stats**

Enable or disable flow table statistics update for enforcement applications.

**app-mon flow-table enforcement stats admin-state {enable | disable}**

### Syntax Definitions

- **enable**: Enable flow-table statistics update.
- **disable**: Disable flow-table statistics update.

### Defaults

By default, statistics admin status is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command is applicable only for enforcement applications.
- The statistics collection capability is shared with Service Manager, which means that either the Service Manager feature or AppMon can use this capability at any given time. Hence, disabling the counter usage in Service Manager using the `service stats disable` command is required to view the flow table statistics update for enforcement applications. For more information about this command, see the “Service Manager Commands” chapter in the *OmniSwitch AOS Release 8 CLI Reference Guide*.
- When update statistics is enabled, the updated statistics is displayed in the `show app-mon ipv4-flow-table enforcement verbose`, `show app-mon ipv6-flow-table enforcement verbose`, and `show app-mon app-list enforcement active stats` commands. Statistics are refreshed every 160 seconds from data path, and based on the flow sync interval between the data path and the control path.

### Examples

- `-> app-mon flow-table enforcement stats admin-state enable`
- `-> app-mon flow-table enforcement stats admin-state disable`

### Release History

Release 8.2.1; command introduced.
Related Commands

show app-mon config          Displays global AppMon configuration.

MIB Objects

alaAppMonEnforcementFlowTableStatsAdminStatus
app-mon aging enforcement

Configures aging time for dynamically learned TCP/UDP flows for each application for Enforcement applications.

app-mon aging enforcement app-name app_name [tcp | udp] interval {120m | 60m | 30m | 10m | 5m | 3m | default}

Syntax Definitions

app_name
Name of the application to configure its aging interval. The application must be part of the application pool.

interval
The aging time interval for dynamically learned flows in the flow table, in minutes.

default
Configures the default aging interval.

Defaults

By default, aging interval is set per application and TCP or UDP flow type basis.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- User can set separate TCP or UDP flows aging interval for an given application.
- When TCP option is used to configure aging interval for an application, TCP flows generated by a given application age out with configured value.
- When UDP option is used to configure aging interval for an application, UDP flows generated by a given application age out with configured value.
- Flow aging is supported for the applications that are part of the enforcement application list. Flows related with enforcement application list are made active for QoS treatment as well statistics collection.
- Flow aging is not supported for applications that are part of Monitor application list. Monitor flow tables log these flows when they are detected until logging threshold is reached.

Examples

-> app-mon aging enforcement app-name sip tcp interval 60m
-> app-mon aging enforcement app-name tftp udp interval 120m
Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config
Displays global AppMon configuration.

show app-mon aging enforcement
Displays the aging interval for each application for enforcement feature.

MIB Objects

alaAppMonEnforcementAgingTimerTable
alaAppMonEnforcementAgingTimerValue
**app-mon logging-threshold**

Configures the threshold for the number of matched flows for enforcement and monitor applications.

```
app-mon logging-threshold {enforcement | monitor} num-of-flows {number | default}
```

**Syntax Definitions**

- **number**: Threshold value for the number of matched flows. The valid range is 1000–60000.
- **default**: Sets the threshold back to the default value of 20K.

**Defaults**

By default, 20000 flows are logged.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the logging threshold value is set to ‘0’, flows are not logged to the log file.
- When used with enforcement option, it configures the threshold for the number of matched flows to be saved on the log file for enforcement applications.
- When used with monitor option, it configures the threshold for the number of matched flows to be displayed in the monitor flow table commands.

**Examples**

```
-> app-mon logging-threshold monitor num-of-flows 10000
-> app-mon logging-threshold monitor num-of-flows default
-> app-mon logging-threshold enforcement num-of-flows 10000
```

**Release History**

Release 8.2.1; command introduced.

**Related Commands**

- `show app-mon config` Displays global AppMon configuration.
MIB Objects

alaAppMonThresholdNumberOfFlows
**app-mon flow-sync enforcement interval**

Configures the interval at which the enforcement flows information is refreshed.

```
app-mon flow-sync enforcement interval {number | default}
```

**Syntax Definitions**

- **number**: Flow sync interval at which the enforcement flows information is refreshed. The valid range is 10–3600 seconds. The interval can be configured only for the enforcement feature.

- **default**: Configures the default flow-sync interval.

**Defaults**

Default flow-sync interval is 60 seconds for enforcement.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The refreshed information is shown in the following show commands: `show app-mon applist enforcement active`, `show app-mon applist enforcement active stats`, `show app-mon ipv4-flow-table enforcement`, `show app-mon stats`.

**Examples**

```
-> app-mon flow-sync enforcement interval 10
-> app-mon flow-sync enforcement interval default
```

**Release History**

Release 8.2.1; command introduced.
**Related Commands**

- `show app-mon ipv4-flow-table`  Displays the flow table for IPv4 flows entries.
- `show app-mon ipv6-flow-table`  Displays the flow table for IPv6 flows entries.

**MIB Objects**

- `alaAppMonFlowSyncEnforcementInterval`
**app-mon force-flow-sync**

Synchronizes flows learned in the data path.

`app-mon force-flow-sync {enforcement | monitor}`

---

**Syntax Definitions**

- **enforcement**: Synchronizes flows learned in the data path for the enforcement feature from the hardware.
- **monitor**: Synchronizes flows learned in the data path for the monitor feature from the hardware.

---

**Defaults**

By default, flow synchronization occurs every 5 minutes for monitor flows and 60 seconds for enforcement flows.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use this command to force a flow synchronization with the control path database in real time.

---

**Examples**

```
-> app-mon force-flow-sync enforcement
-> app-mon force-flow-sync monitor
```

---

**Release History**

Release 8.2.1; command introduced.

---

**Related Commands**

- `show app-mon ipv4-flow-table` Displays the flow table for IPv4 flows entries.
- `show app-mon ipv6-flow-table` Displays the flow table for IPv6 flows entries.

---

**MIB Objects**

- `alaAppMonForceFlowSyncStatus`
**app-mon separate-config-file**

Reduces the per-application level AppMon configuration display in the `show configuration snapshot` output as well as in “vcboot.cfg”.

`app-mon separate-config-file`

`no app-mon separate-config-file`

---

**Syntax Definitions**

N/A

**Defaults**

By default, the separate configuration file option is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

|--------------|------|------|------|-------|------|-------|------|------|--------------|                |             |        |      |------|------|
|              | No   | No   | No   | No    | Yes  | Yes   | No   | No   | No           | No             | No            | No            | No     | No   | No   |

**Usage Guidelines**

- When this command is used, per-application level AppMon configuration is moved to a separate file called “appmon_vcboot.cfg” from “vcboot.cfg” on write memory.
- Use the `no` form of this command to disable the separate configuration file feature.

**Examples**

```
-> app-mon separate-config-file
-> no app-mon separate-config-file
```

**Release History**

Release 8.7R1; command introduced.

**Related Commands**

- `show app-mon config` Displays global AppMon configuration.

**MIB Objects**

- `alaAppMonSeparateConfigFile`
**app-mon data**

Provides an option to extract pre-defined attributes of a given application for debugging and monitoring purposes. Use this command to view the interface information for an application attribute flow.

```
app-mon data app_name [filter filter_header | no-page]
```

**Syntax Definitions**

- **app_name**: Name of the application from which to extract pre-defined attributes.
- **filter_header**: Filter the data attributes based on various fields like time, interface, source MAC, destination MAC and so on.
- **no-page**: Filter with this option to display all the records.

**Default**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570/M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>X48C6/T48C6</td>
<td>X48C4E/V48C8</td>
<td>C32E/T24C2</td>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This is a meta CLI, and does not have corresponding SNMP MIB object.
- This command does not allow any configuration; can be used to view the attribute records for a specific application. Currently, this command can be used only for **IEC104** application.
- The data attributes can be filtered based on various fields like time, interface, source MAC, destination MAC and so on. Filter with ‘no-page’ option to display all the records.

**Examples**

```
-> app-mon data
Please wait...
Usage: app-mon data <app-name> [filter "string"] [no-page]
app-name: display attribute records of an application name
filter: to display attribute records based on given column name (s)
no-page: display all the attribute records
Filter Usage: app-mon data <app-name> filter "ColumnNmael=value1, ColumnN-
name2=value2 ..." [no-page]
Header:
Time | Interface | SrcMac | SrcIp | SrcPort | DesMac | DesIp | DesPort | CauseTx | acpi_type | acpi_utype | asdu | Total
```

OmniSwitch AOS Release 8 CLI Reference Guide    April 2023    page 41-34
Examples:

app-mon data <app-name> filter "interface=1/1/18"
app-mon data <app-name> filter "interface=1/1/18, SrcIp= 135.254.163.134"

Example 1:

```plaintext
-> app-mon data iec104
Please wait...
```

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>SrcMac</th>
<th>SrcIp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SrcPort</td>
<td>DesMac</td>
<td>DesIp</td>
<td>DesPort</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/2/2020 7:09</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Press any key to continue or 'q' to quit:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 2:

```plaintext
-> app-mon data iec104 filter "DesIp=1.1.1.2, acpi_type=3"
Please wait...
```

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>SrcMac</th>
<th>SrcIp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SrcPort</td>
<td>DesMac</td>
<td>DesIp</td>
<td>DesPort</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Press any key to continue or 'q' to quit:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 3:

```plaintext
-> app-mon data iec104 filter "DesIp=1.1.1.2, acpi_type=3" no-page
Please wait...
```

<table>
<thead>
<tr>
<th>Time</th>
<th>Interface</th>
<th>SrcMac</th>
<th>SrcIp</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SrcPort</td>
<td>DesMac</td>
<td>DesIp</td>
<td>DesPort</td>
</tr>
<tr>
<td>-----------</td>
<td>--------</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>4/2/2020 7:08</td>
<td>1/1/2011</td>
<td>00:01:01:01:01:00</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td>00:01:01:01:00:00</td>
<td>1.1.1.2</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td>Press any key to continue or 'q' to quit:</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Release History

Release 8.7R1; command introduced.

Related Commands
N/A

MIB Objects
N/A
**app-mon enforcement-mode**

Enables the enforcement for either IPv4 or IPv4-IPv6 flows.

```plaintext
app-mon enforcement-mode [ipv4 | ipv4-ipv6]
```

### Syntax Definitions

- **ipv4**  
  Applies enforcement to IPv4 flows.

- **ipv4-ipv6**  
  Applies enforcement to IPv4-IPv6 flows.

### Default

By default, enforcement mode is set to IPv4-IPv6.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6465</th>
<th>6560</th>
<th>6860</th>
<th>6570M</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>IPv4-IPv6</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enforcement mode can be changed only when AppMon is in disabled state.
- Enforcement mode does not apply to monitoring app-list.
- Enforcement mode is specific to enforcement app-list only. However, this configuration does not impact the flow matching or tracking of IPv4 and IPv6 flows for applications that are part of enforcement app-lists; it only affects the subsequent QoS enforcement for flows.
- If mode is IPv4, QoS enforcement is not supported for the IPv6 flows; however, flow matching and tracking will be supported for IPv6 flows.
- If mode is IPv4-IPv6, flow matching, tracking, and QoS enforcement are supported for both IPv4 and IPv6 flows.
- This configuration is to enable user to increase the number of flows supported for QoS enforcement. User can increase number of flows supported for QoS enforcement by configuring IPv4 mode. However, it will not support QoS enforcement for IPv6 flows.

### Examples

```plaintext
-> app-mon enforcement-mode ipv4
-> app-mon enforcement-mode ipv4-ipv6
```

### Release History

Release 8.7R2; command introduced.
Related Commands

show app-mon config Displays global AppMon configuration.

MIB Objects

alaAppMonConfig
    alaAppMonEnforcementMode
**show app-mon config**

Displays global AppMon configuration.

*show app-mon config [app-snapshot]*

---

**Syntax Definitions**

`app-snapshot` Displays per-application level AppMon configuration.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The operational state is enabled if there is at least one OmniSwitch 6860E chassis in the virtual chassis (VC). If there is no OmniSwitch 6860E in the VC, the operational-state is disabled.
- Use `app-snapshot` option to view the AppMon configuration at an application level.

---

**Examples**

```shell
-> show app-mon config
Admin State                      : Enable,
Operational State                : Enable,
Separate Config File Status      : Yes,
L3-IPv4                          : Enable,
L3-IPv6                          : Enable,
Enforcement Flow-Table Stats     : Enable,
Enforcement Flow-Sync Interval   : 60 seconds,
Monitor Logging Threshold        : 7000,
Enforcement Logging Threshold    : 7000,
App-Pool Applications            : 2849,
Monitor Applied Applications     : 2849,
Enforcement Applied Applications : 2849,
Upgraded Signature File Type     : Production,
AOS Compatible Signature Kit Version : 1,
Signature Kit version            : 3.7.6

-> show app-mon config app-snapshot
! APP-MONITORING:
  app-mon app-group "Web" add app-name "01net"
```
show app-mon config

Admin State : Enable,
Operational State : Enable,
Separate Config File Status : Yes,
Enforcement Mode : IPV4-IPV6,
Enforcement Flow-Sync Interval : 60 seconds,
Monitor Logging Threshold : 7000,
Enforcement Logging Threshold : 7000,
App-Pool Applications : 2849,
Monitor Applied Applications : 2849,
Enforcement Applied Applications : 2849,
Upgraded Signature File Type : Production,
AOS Compatible Signature Kit Version : 1,
Signature Kit version : 3.7.6

**output definitions**

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin-state</td>
<td>The AppMon administrative status (Enabled or Disabled). Configured through the app-mon admin-state command.</td>
</tr>
<tr>
<td>Operational State</td>
<td>The operational status (Enabled or Disabled).</td>
</tr>
<tr>
<td>Separate Config File Status</td>
<td>Separate configuration file status (Yes or No).</td>
</tr>
<tr>
<td>Enforcement Mode</td>
<td>The enforcement mode set. (IPv4 or IPv4-IPv6).</td>
</tr>
<tr>
<td>Enforecement Flow-Sync Interval</td>
<td>Status of the enforcement flow table statistics update.</td>
</tr>
<tr>
<td>Monitor Logging-Threshold</td>
<td>Monitor threshold value for the flows to be saved in the IPv4 or IPv6 flow table.</td>
</tr>
<tr>
<td>Enforcement Logging-Threshold</td>
<td>Enforcement threshold value for the flows to be saved into the log file.</td>
</tr>
<tr>
<td>L3-IPv4</td>
<td>Status of IPv4 l3 mode on the switch (Enable or Disable).</td>
</tr>
<tr>
<td>L3-IPv6</td>
<td>Status of IPv6 l3 mode on the switch (Enable or Disable).</td>
</tr>
<tr>
<td>Enforcement Flow Table Stats</td>
<td>Enforcement flow sync interval at which the switch polls for flow information.</td>
</tr>
<tr>
<td>AOS Compatible Signature Kit Version</td>
<td>Determines the compatibility between AOS software and the signature file.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.2.1; command introduced.
Release 8.7R1; **app-snapshot** keyword added, “Separate Config File Status” field added.
Release 8.7R2; “Enforcement Mode” field added.

**Related Commands**

```
show app-mon port
```
Displays AppMon status per physical port or per slot.

**MIB Objects**

- `alaAppMonAdminStatus`
- `alaAppMonOperStatus`
- `alaAppMonAgingInterval`
- `alaAppMonAppliedApplications`
- `alaAppMonAppPoolApplications`
- `alaAppMonSignatureFileVersion`
- `alaAppMonLoggingThreshold`
- `alaAppMonKitCompatatabilityVersion`
- `alaAppMonAOSCompatatabilityVersion`
- `alaAppMonAutoGroupCreation`
show app-mon port

Displays AppMon status per physical port or per slot for the switch.

show app-mon [port chassis/slot/port | slot chassis/slot]

Syntax Definitions

chassis/slot/port[\-port2]  The chassis ID, slot, and port number (3/1/1) for a specific port. Use a hyphen to specify a range of ports (3/1/1-8).

chassis/slot  The chassis ID and slot number (3/1) for a specific slot.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8</th>
<th>6900C32E/T24C2</th>
<th>9900X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show app-mon port

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin-Status</th>
<th>Oper-Status</th>
<th>L4-mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/4</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/6</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/7</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
</tbody>
</table>

-> show app-mon slot 1/1

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin-Status</th>
<th>Oper-Status</th>
<th>L4-mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/2</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/3</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
</tbody>
</table>
show app-mon port

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin-Status</th>
<th>Oper-Status</th>
<th>L4-mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/4</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/5</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/6</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/7</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
<tr>
<td>1/1/8</td>
<td>Enable</td>
<td>Up</td>
<td>TCP-UDP</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>Admin-Status</th>
<th>Oper-Status</th>
<th>L4-mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The chassis identifier, slot, and port on which AppMon is enabled or disabled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin-Status</td>
<td>Indicates the admin status of the port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oper-Status</td>
<td>Indicates the operational status of the port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L4-mode</td>
<td>Indicates the L4 mode: TCP or UDP.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config  Displays global AppMon configuration.

MIB Objects

alaAppMonPortConfigTable
   alaAppMonPortConfigSlotPortIndex
   alaAppMonPortConfigPortStatus
   alaAppMonPortConfigPortOperStatus
   alaAppMonPortConfigPortType
show app-mon app-pool

Displays all the applications that are part of an application pool.

show app-mon app-pool

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show app-mon app-pool

Legend: Application-name: *= Not present in recently updated kit,

<table>
<thead>
<tr>
<th>AppId</th>
<th>Application-name</th>
<th>Revision</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>968</td>
<td>amazon</td>
<td>1.0.0</td>
<td>Web</td>
</tr>
<tr>
<td>244</td>
<td>facebook</td>
<td>1.0.0</td>
<td>Web</td>
</tr>
<tr>
<td>182</td>
<td>sip</td>
<td>1.0.0</td>
<td>Audio/Video</td>
</tr>
<tr>
<td>183</td>
<td>skype</td>
<td>1.1.0</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>211</td>
<td>tftp</td>
<td>1.0.0</td>
<td>File Server</td>
</tr>
<tr>
<td>503</td>
<td>twitter</td>
<td>1.0.0</td>
<td>Web</td>
</tr>
<tr>
<td>597</td>
<td>viber</td>
<td>1.0.0</td>
<td>Audio/Video</td>
</tr>
<tr>
<td>890</td>
<td>viber</td>
<td>1.0.0</td>
<td>Audio/Video</td>
</tr>
<tr>
<td>1093</td>
<td>whatsapp</td>
<td>1.0.0</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>240</td>
<td>youtube</td>
<td>1.0.0</td>
<td>Web</td>
</tr>
</tbody>
</table>
Number of Applications: 10

output definitions

<table>
<thead>
<tr>
<th>AppId</th>
<th>Identity of the application group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-name</td>
<td>Name of the application group whose details are viewed.</td>
</tr>
<tr>
<td>Note: * indicates that the application is not present in the recently updated signature file.</td>
<td></td>
</tr>
<tr>
<td>Revision</td>
<td>Application revision number.</td>
</tr>
<tr>
<td>Category</td>
<td>Application category name.</td>
</tr>
</tbody>
</table>

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config Displays global AppMon configuration.

MIB Objects

alaAppMonAppPoolTable
  alaAppMonAppPoolAppName
  alaAppMonAppPoolCategory
  alaAppMonAppPoolRevision
  alaAppMonAppPoolAppStatus
**show app-mon app-list**

Displays a list of applications and application groups added to an application list.

```
show app-mon app-list {monitor | enforcement} [active [stats]|conflict]
```

### Syntax Definitions

- **monitor**: Displays information for applications added for monitoring.
- **enforcement**: Displays information for applications added for enforcement.
- **active [stats]**: Displays the list of activated applications in an application list. Use the `stats` option together with the `enforcement` option.
- **conflict**: Displays the list of applications that are present more than once in an application list.

### Defaults

By default, all applications and application groups that belong to an application list are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **conflict** option to identify applications that are present more than once in an application list. This needs to be checked and resolved for **app-mon apply** to be successful.
- The **active** option displays active and gross number of flows detected on per application basis.
- For monitor feature, **active** option displays only the gross counters.
- The **stats** option is used only for the **enforcement** option. This displays active or gross packets/byte counters per application basis.
### Examples

-> show app-mon app-list monitor

<table>
<thead>
<tr>
<th>App-Id/ AppGrp-Id</th>
<th>Application-List Member Name</th>
<th>Application-List Member Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>244</td>
<td>facebook</td>
<td>APP</td>
</tr>
<tr>
<td>182</td>
<td>sip</td>
<td>APP-GRP</td>
</tr>
</tbody>
</table>

#### output definitions

- **App-Id/AppGrp-Id**: Identity of the application or application group.
- **Application-List Member Name**: Name of the application group or application.
- **Application-List Member Type**: Specifies the application type: individual application or whether the application belongs to any application group.

-> show app-mon app-list monitor active

Legend: Application-name: *= Not present in recently updated kit,

<table>
<thead>
<tr>
<th>App-ID</th>
<th>Application Name</th>
<th>App-Grp Name</th>
<th>Matched Gross Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>968</td>
<td>amazon</td>
<td>APP</td>
<td>0</td>
</tr>
<tr>
<td>244</td>
<td>facebook</td>
<td>APP</td>
<td>0</td>
</tr>
<tr>
<td>211</td>
<td>tftp</td>
<td>APP-GRP</td>
<td>24508</td>
</tr>
</tbody>
</table>

Number of Applications: 3

#### output definitions

- **App-ID**: Identity of the application group.
- **Application Name**: Name of the application.
- **App-Grp Name**: Name of the application group.
- **Matched Gross Count**: Total number of matched active flows per application.
- **Number of Applications**: Total number of active applications in the application list.

-> show app-mon app-list monitor conflict

<table>
<thead>
<tr>
<th>Sn</th>
<th>App-ID</th>
<th>Application-Name</th>
<th>Application-Group</th>
<th>Error-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>244</td>
<td>facebook</td>
<td>APP</td>
<td>Duplicate</td>
</tr>
<tr>
<td>2</td>
<td>244</td>
<td>facebook</td>
<td>APP</td>
<td>Duplicate</td>
</tr>
</tbody>
</table>

#### output definitions

- **Sn**: The serial number.
- **App-ID**: Identity of the application group.
- **Application-Name**: Name of the application.
- **Application-Group**: Name of the application group.
- **Error-Type**: Displays the type of error.
-> show app-mon app-list enforcement
Legend: Application-name: * = Not present in recently updated kit,
<table>
<thead>
<tr>
<th>App-Id/AppGrp-Id</th>
<th>Application-List Member Name</th>
<th>Application-List Member Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>244</td>
<td>facebook</td>
<td>grp1</td>
</tr>
</tbody>
</table>

output definitions

**App-Id/AppGrp-Id**
Identity of the application or application group

**Application-List Member Name**
Name of the application group or application.
Note: * indicates that the application is not present in the recently updated signature file.

**Application-List Member Type**
Specifies the application type: individual application or whether the application belongs to any application group.

-> show app-mon app-list enforcement active
Legend: Application-name: * = Not present in recently updated kit,
<table>
<thead>
<tr>
<th>App-Id</th>
<th>Application Name</th>
<th>App-Grp Name</th>
<th>Matched Flow Count</th>
<th>Matched Gross Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>968</td>
<td>amazon</td>
<td>grp1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>182</td>
<td>sip</td>
<td>grp1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>211</td>
<td>tftp</td>
<td>grp1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>890</td>
<td>webex</td>
<td>grp1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1093</td>
<td>whatsapp</td>
<td>grp2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>183</td>
<td>skype</td>
<td>grp1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>597</td>
<td>viber</td>
<td>grp2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>244</td>
<td>facebook</td>
<td>grp1</td>
<td>7837</td>
<td>8192</td>
</tr>
<tr>
<td>503</td>
<td>twitter</td>
<td>grp1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>240</td>
<td>youtube</td>
<td>grp2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Number of Applications: 10

output definitions

**Application Name**
Name of the application.
Note: * indicates that the application is not present in the recently updated signature file.

**App-Id**
Identity of the application group.

**App-Group Name**
Name of the application group.

**Matched Flow Count**
Number of matched active flows per application.

**Matched Gross Count**
Total number of matched flows per application.

**Number of Applications**
Total number of active applications in the application list.
show app-mon app-list enforcement active stats
Legend: Application-name: *= Not present in recently updated kit,

<table>
<thead>
<tr>
<th>App-Id</th>
<th>Application Name</th>
<th>App-Grp</th>
<th>Matched Active Packet Count</th>
<th>Matched Active Byte Count</th>
<th>Matched Gross Packet Count</th>
<th>Matched Gross Byte Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>182</td>
<td>SIP</td>
<td>grp1</td>
<td>1236</td>
<td>15236</td>
<td>1000</td>
<td>15000</td>
</tr>
<tr>
<td>211</td>
<td>TFTP</td>
<td>grp1</td>
<td>2000</td>
<td>345678</td>
<td>3456</td>
<td>604569</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Name of the application. Note: * indicates that the application is not present in the recently updated signature file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>App-Id</td>
<td>Identity of the application group.</td>
</tr>
<tr>
<td>App-Group Name</td>
<td>Name of the application group.</td>
</tr>
<tr>
<td>Matched Active Packet Count</td>
<td>Packet count of active matched flows.</td>
</tr>
<tr>
<td>Matched Active Byte Count</td>
<td>Byte count of active matched flows</td>
</tr>
<tr>
<td>Matched Gross Packet Count</td>
<td>Cumulative packet count of active matched flows and ended flows.</td>
</tr>
<tr>
<td>Matched Gross Byte Count</td>
<td>Cumulative byte count of active matched flows and ended flows.</td>
</tr>
</tbody>
</table>

show app-mon app-list enforcement conflict

<table>
<thead>
<tr>
<th>Sn</th>
<th>App-ID</th>
<th>Application-Name</th>
<th>Application-Group</th>
<th>Error-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>244</td>
<td>facebook</td>
<td>grp1</td>
<td>Duplicate</td>
</tr>
<tr>
<td>2</td>
<td>244</td>
<td>facebook</td>
<td>grp1</td>
<td>Duplicate</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Sn</th>
<th>The serial number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>App-ID</td>
<td>Identity of the application group.</td>
</tr>
<tr>
<td>Application-Name</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>Application-Group</td>
<td>Name of the application group.</td>
</tr>
<tr>
<td>Error-Type</td>
<td>Displays the type of error.</td>
</tr>
</tbody>
</table>

Release History

Release 8.2.1; command introduced.

Related Commands

- show app-mon config Displays global AppMon configuration.
- show app-mon app-group Displays the details of all the applications in an application group.
### MIB Objects

alaAppMonActiveAppListTable
  alaAppMonActiveAppListMemberName
  alaAppMonActiveAppListMemberType
  alaAppMonActiveAppListMemberStatus
  alaAppMonActiveAppListAppId
  alaAppMonActiveAppListAppStatus

alaAppMonActiveAppListTable
  alaAppMonActiveAppListAppName
  alaAppMonActiveAppListAppGroupName
  alaAppMonActiveAppListAppId
  alaAppMonActiveAppListAppStatus

alaAppMonAppListConflictTable
  alaAppMonAppListConflictIndex
  alaAppMonAppListConflictAppName
  alaAppMonAppListConflictAppId
  alaAppMonAppListConflictAppGroupName
  alaAppMonAppListConflictErrorType

alaAppMonEnforcementAppListTable
  alaAppMonEnforcementAppListMemberName
  alaAppMonEnforcementAppListAppOrGroupID
  alaAppMonEnforcementAppListMemberType
  alaAppMonEnforcementAppListAppStatus

alaAppMonEnforcementActiveAppListTable
  alaAppMonEnforcementActiveAppListAppName
  alaAppMonEnforcementActiveAppListAppGroupName
  alaAppMonEnforcementActiveAppListAppOrGroupID
  alaAppMonEnforcementActiveAppListTotalMatchedFlows
  alaAppMonEnforcementActiveAppListActiveMatchedFlows
  alaAppMonEnforcementActiveAppListAppID
  alaAppMonEnforcementActiveAppListAppStatus
  alaAppMonEnforcementActiveAppListActivePktCount
  alaAppMonEnforcementActiveAppListActiveByteCount
  alaAppMonEnforcementActiveAppListGrossPktCount
  alaAppMonEnforcementActiveAppListGrossByteCount

alaAppMonEnforcementAppListConflictTable
  alaAppMonEnforcementAppListConflictIndex
  alaAppMonEnforcementAppListConflictAppID
  alaAppMonEnforcementAppListConflictAppName
  alaAppMonEnforcementAppListConflictAppGroupName
  alaAppMonEnforcementAppListConflictAppErrorType
**show app-mon app-group**

Displays the details of all the applications in an application group.

`show app-mon app-group [group-name group_name]`

**Syntax Definitions**

`group_name` The name of an application group. This is a case sensitive string.

**Defaults**

By default, information is displayed for all application groups.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command displays both user created and automatically created application groups and the applications added to the respective group.
- Application names which are added to group and not yet activated are also displayed.
- This also display the auto application groups.

**Examples**

```
-> show app-mon app-group
Legend: Application-name: * = Not present in recently updated kit,
AppGrp-Id App-group App-name
----------------------------------------+----------------------------------------+
AG-1 Web  amazon                      
AG-1 Web  facebook                    
AG-1 Web  twitter                     
AG-1 Web  youtube                     
AG-1 Web  whatsapp                    
AG-1 Web  skype                       
AG-1 Web  sip                         
AG-1 Web  viber                       
AG-1 Web  webex                       
AG-2 Instant Messaging                 
AG-3 Audio/Video                      
```

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 41-51
### Show Application Group Details

**Output Definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AppGrp-Id</td>
<td>Identity of the application group.</td>
</tr>
<tr>
<td>App-group</td>
<td>Name of the application group whose details are viewed.</td>
</tr>
<tr>
<td>App-name</td>
<td>Name of the applications attached to the application group.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.2.1; command introduced.

**Related Commands**

- `show app-mon config`: Displays global AppMon configuration.
- `show app-mon app-list`: Displays list of applications and application groups added to an application list.

**MIB Objects**

- `alaAppMonAppGroupTable`
  - `alaAppMonAppGroupName`
  - `alaAppMonAppGroupMember`
  - `alaAppMonAppGroupCategoryName`
  - `alaAppMonAppGrpId`
  - `alaAppMonAppGroupAppStatus`
  - `alaAppMonAppGroupStatus`
show app-mon app-record

Displays current-hour application-record information as well the historic application-records on the hourly or 24-hours basis for monitored applications.

show app-mon app-record [hourly | twenty-four-hours | current-hour] [verbose]

**Syntax Definitions**

- **hourly**
  Displays flows detected for an application in an hour. An Hour is defined with fixed boundary (for example, 1:30 p.m to 2:30 p.m).

- **twenty-four-hours**
  Displays aggregate of available 'hourly' records for each application, flows detected in last 24-hours since last hour boundary. 'current-hour' data will not be part of this. This information is updated every one hour when 'hourly' record is updated.

- **current-hour**
  Displays new flow detected for an application in the current hour which is not part of 'hourly' historic data. When current-hour reaches an hour boundary, this data is moved to 'hourly' records. For example, if current time is 2.40 p.m, then information between 2.30 p.m to 2.40 p.m is displayed. On 3.30 p.m, current-hour information is moved to the latest hourly record.

- **verbose**
  Select this option to view detail information for each option. Detail information include minimum, maximum and average flows detected for each application.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This is supported for monitoring.

**Examples**

```
-> show app-mon app-record current-hour
Sampling Interval Every 5-minutes
Application                          Application group     Total Detected Flows
------------------------------------+-------------------+----------------------
2015-07-28 15:30:00 IST 0d 00h 48m 11s
sip                                 grp1                 11
```
<table>
<thead>
<tr>
<th>Application</th>
<th>Application group</th>
<th>Total Detected Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>youtube</td>
<td>grp1</td>
<td>16572</td>
</tr>
</tbody>
</table>

Number of Applications: 2

-> show app-mon app-record hourly
Sampling Interval Every 5-minutes

<table>
<thead>
<tr>
<th>Application</th>
<th>Application group</th>
<th>Total Detected Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>youtube</td>
<td>grp1</td>
<td>21534</td>
</tr>
</tbody>
</table>

Number of Applications: 2

---

<table>
<thead>
<tr>
<th>Application</th>
<th>Application group</th>
<th>Total Detected Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>facebook</td>
<td>grp2</td>
<td>24</td>
</tr>
</tbody>
</table>

Number of Applications: 1

---

Number of hourly App-Records: 2

-> show app-mon app-record hourly verbose
Sampling Interval Every 5-minutes

<table>
<thead>
<tr>
<th>Application</th>
<th>Application group</th>
<th>Min.</th>
<th>Max.</th>
<th>Avg.</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>facebook</td>
<td>grp2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>youtube</td>
<td>grp1</td>
<td>1184</td>
<td>12600</td>
<td>7178</td>
<td>21534</td>
</tr>
</tbody>
</table>

Number of Applications: 2

---

<table>
<thead>
<tr>
<th>Application</th>
<th>Application group</th>
<th>Total Detected Flows</th>
</tr>
</thead>
<tbody>
<tr>
<td>facebook</td>
<td>grp2</td>
<td>4</td>
</tr>
</tbody>
</table>

Number of Applications: 1

---

Number of hourly App-Records: 2
-> show app-mon app-record twenty-four-hours
Sampling Interval Every 5-minutes
2015-10-09 12:30:00 IST 1d 00h 00m 00s

<table>
<thead>
<tr>
<th>Application</th>
<th>Total Detected Flows (24-hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>skype</td>
<td>471</td>
</tr>
<tr>
<td>youtube</td>
<td>4239</td>
</tr>
<tr>
<td>facebook</td>
<td>102</td>
</tr>
<tr>
<td>twitter</td>
<td>2</td>
</tr>
<tr>
<td>viber</td>
<td>99</td>
</tr>
<tr>
<td>whatsapp</td>
<td>13</td>
</tr>
</tbody>
</table>

Number of Applications: 6

-> show app-mon app-record twenty-four-hours verbose
Sampling Interval Every 5-minutes
2015-10-09 12:30:00 IST 1d 00h 00m 00s

<table>
<thead>
<tr>
<th>Application</th>
<th>Detected Flows (24-hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min.</td>
</tr>
<tr>
<td>skype</td>
<td>2</td>
</tr>
<tr>
<td>youtube</td>
<td>1</td>
</tr>
<tr>
<td>facebook</td>
<td>4</td>
</tr>
<tr>
<td>twitter</td>
<td>2</td>
</tr>
<tr>
<td>viber</td>
<td>1</td>
</tr>
<tr>
<td>whatsapp</td>
<td>1</td>
</tr>
</tbody>
</table>

Number of Applications: 6

**output definitions**

<table>
<thead>
<tr>
<th>Application</th>
<th>Name of the application.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application group</td>
<td>Name of the application group.</td>
</tr>
<tr>
<td>Detected Flows</td>
<td><strong>Min:</strong> Minimum number of flows that were detected. <strong>Max:</strong> Maximum number of flows that were detected. <strong>Avg:</strong> Average number of flows that were detected. <strong>Total:</strong> Total number of flows that were detected.</td>
</tr>
<tr>
<td>Number of Applications</td>
<td>Displays the total number of applications.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.2.1; command introduced.
Related Commands

`show app-mon config` Displays the global AppMon configuration.

MIB Objects

`alaAppMonAppRecCurrentHrStatsTable`
- `alaAppMonAppRecCurrentHrStatsName`
- `alaAppMonAppRecCurrentHrStatsMinActiveFlow`
- `alaAppMonAppRecCurrentHrStatsMaxActiveFlow`
- `alaAppMonAppRecCurrentHrStatsAvgActiveFlow`
- `alaAppMonAppRecCurrentHrStatsTotalFlow`

`alaAppMonAppRecHrlyStatsTable`
- `alaAppMonAppRecHrlyStatsName`
- `alaAppMonAppRecHrlyStatsMinActiveFlow`
- `alaAppMonAppRecHrlyStatsMaxActiveFlow`
- `alaAppMonAppRecHrlyStatsAvgActiveFlow`
- `alaAppMonAppRecHrlyStatsTotalFlow`

`alaAppMonAppRec24HrStatsTable`
- `alaAppMonAppRec24HrStatsName`
- `alaAppMonAppRec24HrStatsMinActiveFlow`
- `alaAppMonAppRec24HrStatsMaxActiveFlow`
- `alaAppMonAppRec24HrStatsAvgActiveFlow`
- `alaAppMonAppRec24HrStatsTotalFlow`
**show app-mon ipv4-flow-table**

Displays the flow table for IPv4 flows entries for enforcement and monitor flows.

`show app-mon ipv4-flow-table {monitor | enforcement [verbose]} [{src-ipv4 | dest-ipv4} ip_address] [app-name app_name | app-group grp_name]`

---

**Syntax Definitions**

- **verbose**
  - Displays detailed information of the flows.

- **src-ipv4 ip_address**
  - Filter flow table based on the specified source IPv4 address.

- **dest-ipv4 ip_address**
  - Filter flow table based on the specified destination IPv4 address.

- **app_name**
  - Filter flow table based on application name.

- **grp_name**
  - Filter flow table based on application group.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The **verbose** option displays additional information about the flow start time, statistics counters, associated application group, policy rule, and so on. This option is supported only for enforcement feature.

- On OmniSwitch 6860N, flows will take ten minutes to age out when the flow is idle.

**Examples**

```
-> show app-mon ipv4-flow-table monitor
SrcIP        DestIP        SrcPort  DestPort  Proto  App Name  App Group
------------------------------------------+-----------------------------------+----------+----------+---------+----------+----------
100.0.0.10   101.0.0.10   48128    3128     TCP     facebook test
100.0.0.10   101.0.0.10   48384    3128     TCP     facebook test
100.0.0.10   101.0.0.10   48640    3128     TCP     facebook test
100.0.0.10   101.0.0.10   48896    3128     TCP     facebook test
```

show app-mon ipv4-flow-table

-> show app-mon ipv4-flow-table monitor src-ipv4 103.20.92.80

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>sPort</th>
<th>dPort</th>
<th>Proto</th>
<th>App Name</th>
<th>App-Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>103.20.92.80</td>
<td>192.168.1.3</td>
<td>443</td>
<td>61069</td>
<td>TCP</td>
<td>whatsapp</td>
<td>test</td>
</tr>
</tbody>
</table>

Number of flows : 1

-> show app-mon ipv4-flow-table monitor dest-ipv4 74.112.124.120

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>sPort</th>
<th>dPort</th>
<th>Proto</th>
<th>App Name</th>
<th>App-Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>209.226.67.175</td>
<td>74.112.124.120</td>
<td>2458</td>
<td>9673</td>
<td>TCP</td>
<td>whatsapp</td>
<td>test</td>
</tr>
</tbody>
</table>

Number of flows : 1

-> show app-mon ipv4-flow-table monitor app-name youtube

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>sPort</th>
<th>dPort</th>
<th>Proto</th>
<th>App Name</th>
<th>App-Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>207.219.97.56</td>
<td>74.125.225.0</td>
<td>1410</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
</tbody>
</table>

Number of flows : 1

output definitions

- **SrcIP**: Displays flow table based on the specified source IPv4 IP address.
- **DestIP**: Displays flow table based on the specified destination IPv4 IP address.
- **SrcPort**: Source port of the flow entry.
- **DestPort**: Destination port of the flow entry.
- **Proto**: Indicates the protocol type (TCP or UDP).
- **App Name**: Displays the flow table based on the application name.
- **App-Group**: Displays the flow table based on the application group.

-> show app-mon ipv4-flow-table enforcement

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>SrcPort</th>
<th>DestPort</th>
<th>Proto</th>
<th>App Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48128</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48384</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48640</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48896</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49152</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49408</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49664</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49920</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
</tr>
</tbody>
</table>

-> show app-mon ipv4-flow-table enforcement verbose

Legend: start/date/time/zone  duration  Packet Count  Byte Count

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>SrcPort</th>
<th>DestPort</th>
<th>Protocol</th>
<th>Application-name</th>
<th>App-group Policy rule Packet Count Byte Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48128</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48384</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48640</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>48896</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49152</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49408</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49664</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
<tr>
<td>100.0.0.10</td>
<td>101.0.0.10</td>
<td>49920</td>
<td>3128</td>
<td>TCP</td>
<td>facebook</td>
<td>test</td>
</tr>
</tbody>
</table>
100.0.0.10 101.0.0.10 49408   3128     TCP       facebook         test     app-mon1      0            0
2015-07-24/15:01:45/IST     0d 0h 1m 31s.

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcIP</td>
<td>Source IPv4 address of the flow.</td>
</tr>
<tr>
<td>DestIP</td>
<td>Destination IPv4 address of the flow.</td>
</tr>
<tr>
<td>SrcPort</td>
<td>Source port of the flow entry.</td>
</tr>
<tr>
<td>DestPort</td>
<td>Destination port of the flow entry.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Indicates the protocol type (TCP or UDP)</td>
</tr>
<tr>
<td>Application Name</td>
<td>Name of the application.</td>
</tr>
<tr>
<td>App-group</td>
<td>Name of the application group.</td>
</tr>
<tr>
<td>Policy rule</td>
<td>The QoS policy applied for enforcement.</td>
</tr>
<tr>
<td>Packet Count</td>
<td>Number of packet counts that match a flow table entry in the hardware.</td>
</tr>
<tr>
<td>Byte Count</td>
<td>Number of byte counts that match a flow table entry in the hardware.</td>
</tr>
</tbody>
</table>

Release History

Release 8.2.1; command introduced.

Related Commands

show app-mon config  Displays global AppMon configuration.

MIB Objects

alaAppMonFlowTable
   alaAppMonFlowSourceIPType
   alaAppMonFlowSourceIP
   alaAppMonFlowDestIPType
   alaAppMonFlowDestIP
   alaAppMonFlowSrcPort
   alaAppMonFlowDestPort
   alaAppMonFlowProtocol
   alaAppMonFlowAppName

alaAppMonEnforcementFlowTable
   alaAppMonEnforcementFlowSourceIPType
   alaAppMonEnforcementFlowSourceIP
   alaAppMonEnforcementFlowDestIPType
   alaAppMonEnforcementFlowDestIP
   alaAppMonEnforcementFlowSrcPort
   alaAppMonEnforcementFlowDestPort
   alaAppMonEnforcementFlowProtocol
   alaAppMonEnforcementFlowAppName
   alaAppMonEnforcementFlowAppGrpName
   alaAppMonEnforcementFlowPolicyRule
   alaAppMonEnforcementFlowStartTime
   alaAppMonEnforcementFlowPktCount
   alaAppMonEnforcementFlowByteCount
**show app-mon ipv6-flow-table**

Displays the flow table for IPv6 flows entries for enforcement and monitor flows.

```
show app-mon ipv6-flow-table {monitor | enforcement [verbose]} [{src-ipv6 | dest-ipv6} ip_address] [app-name app_name | app-group grp_name]
```

### Syntax Definitions

- **verbose**
  Displays detailed information of the flows.

- **src-ipv6 ip_address**
  Filter flow table based on the specified source IPv6 address.

- **dest-ipv6 ip_address**
  Filter flow table based on the specified destination IPv6 address.

- **app_name**
  Filter flow table based on application name.

- **grp_name**
  Filter flow table based on application group.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The **verbose** option displays additional information about the flow start time, statistics counters, associated application group, policy rule, and so on. This option is supported only for enforcement feature.

- On OmniSwitch 6860N, flows will take ten minutes to age out when the flow is idle.

### Examples

```
-> show app-mon ipv6-flow-table monitor
SrcIP   DestIP   SrcPort  DstPort Proto   App Name  App-Group
---------+----------+---------+-------+----------+-----------+---------
1000::14 2000::11      58108    80     TCP   youtube    test
1000::14 2000::11      58364    80     TCP   youtube    test
1000::14 2000::11      57085    80     TCP   youtube    test
1000::14 2000::11      57341    80     TCP   youtube    test
1000::14 2000::11      57597    80     TCP   youtube    test
```

-> show app-mon ipv6-flow-table monitor src-ipv6 1000::11

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Proto</th>
<th>App Name</th>
<th>App-Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>58108</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>58364</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57085</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57341</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57597</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
</tbody>
</table>

Number of flows : 5

-> show app-mon ipv6-flow-table monitor dest-ipv6 2000::11

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Proto</th>
<th>App Name</th>
<th>App-Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>58108</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>58364</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57085</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57341</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57597</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
</tbody>
</table>

Number of flows : 5

-> show app-mon ipv6-flow-table monitor app-group test

<table>
<thead>
<tr>
<th>SrcIP</th>
<th>DestIP</th>
<th>SrcPort</th>
<th>DstPort</th>
<th>Proto</th>
<th>App Name</th>
<th>App-Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>58108</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>58364</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57085</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57341</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>57597</td>
<td>80</td>
<td>TCP</td>
<td>youtube</td>
<td>test</td>
</tr>
</tbody>
</table>

Number of flows : 5

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SrcIP</td>
<td>Displays flow table based on the specified source IPv6 IP address.</td>
</tr>
<tr>
<td>DestIP</td>
<td>Displays flow table based on the specified destination IPv6 IP address.</td>
</tr>
<tr>
<td>SrcPort</td>
<td>Displays the flow table based on the source port.</td>
</tr>
<tr>
<td>DstPort</td>
<td>Displays the flow table based on the destination port.</td>
</tr>
<tr>
<td>Proto</td>
<td>Displays the flow table based on the protocol type.</td>
</tr>
<tr>
<td>App Name</td>
<td>Displays the flow table based on the application name.</td>
</tr>
<tr>
<td>App-Group</td>
<td>Displays the flow table based on the application group.</td>
</tr>
</tbody>
</table>

-> show app-mon ipv6-flow-table enforcement

<table>
<thead>
<tr>
<th>Src IP</th>
<th>Dest IP</th>
<th>App Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>youtube</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>youtube</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>youtube</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>youtube</td>
</tr>
<tr>
<td>1000::14</td>
<td>2000::11</td>
<td>youtube</td>
</tr>
</tbody>
</table>

.
Application Monitoring and Enforcement Commands

```plaintext
-> show app-mon ipv6-flow-table enforcement src-ipv6 1000::14
Src IP                     Dest IP                        App Name
---------------------+-----------------------------+---------------------
1000::14                   2000::11                       youtube
1000::14                   2000::11                       youtube
1000::14                   2000::11                       youtube
1000::14                   2000::11                       youtube
1000::14                   2000::11                       youtube
1000::14                   2000::11                       youtube
```

```plaintext
-> show app-mon ipv6-flow-table enforcement verbose
Legend: start/date/time/zone   duration
SrcIp      DestIP  SrcPort DestPort Protocol Application-name App-group   Policy Rule   Packet Count Byte Count
---------------------------------------------------------------------------------------------------------------
2015-10-11/16:48:55/IST   0d 0h 3m 0s
1000::11  2000::11 61184   80        TCP      youtube           -         appmon-youtube  61           47437
2015-10-11/16:48:56/IST   0d 0h 2m 59s
1000::11  2000::11 61185   80        TCP      youtube           -         appmon-youtube  31           23696
2015-10-11/16:48:57/IST   0d 0h 2m 58s
1000::11  2000::11 61186   80        TCP      youtube           -         appmon-youtube  4            1430
2015-10-11/16:48:58/IST   0d 0h 2m 57s
1000::11  2000::11 61187   80        TCP      youtube           -         appmon-youtube  61           47437
```

Release History

Release 8.2.1; command introduced.

Related Commands

```plaintext
show app-mon config
```

Displays global AppMon configuration.

MIB Objects

```plaintext
alaAppMonFlowTable
  alaAppMonFlowSourceIPType
  alaAppMonFlowSourceIP
  alaAppMonFlowDestIPType
  alaAppMonFlowDestIP
  alaAppMonFlowSrcPort
  alaAppMonFlowDestPort
  alaAppMonFlowProtocol
  alaAppMonFlowAppName
alaAppMonEnforcementFlowTable
  alaAppMonEnforcementFlowSourceIPType
  alaAppMonEnforcementFlowSourceIP
  alaAppMonEnforcementFlowDestIPType
  alaAppMonEnforcementFlowDestIP
  alaAppMonEnforcementFlowSrcPort
  alaAppMonEnforcementFlowDestPort
  alaAppMonEnforcementFlowProtocol
  alaAppMonEnforcementFlowAppName
  alaAppMonEnforcementFlowAppGrpName
  alaAppMonEnforcementFlowPolicyRule
  alaAppMonEnforcementFlowStartTime
  alaAppMonEnforcementFlowPktCount
  alaAppMonEnforcementFlowByteCount
```
show app-mon l4port-exclude

Displays the port range excluded from AppMon operation.

show app-mon l4port-exclude range-id [number]

Syntax Definitions

number A range ID number. The valid range is 1–8.

Defaults

By default, information is displayed for all range ID numbers.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enter a range ID number with this command to display information for a specific range.

Examples

-> show app-mon l4port-exclude range-id

<table>
<thead>
<tr>
<th>Range-Id</th>
<th>Start-port</th>
<th>End-port</th>
<th>Port-type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>200</td>
<td>UDP-Port</td>
</tr>
<tr>
<td>2</td>
<td>20</td>
<td>25</td>
<td>TCP-Service-Port</td>
</tr>
</tbody>
</table>

-> show app-mon l4port-exclude range-id 1

<table>
<thead>
<tr>
<th>Range-Id</th>
<th>Start-port</th>
<th>End-port</th>
<th>Port-type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>100</td>
<td>200</td>
<td>UDP-Port</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range-Id</td>
<td>The service port range ID.</td>
</tr>
<tr>
<td>Start-port</td>
<td>The start port associated with the range ID.</td>
</tr>
<tr>
<td>End-port</td>
<td>The end port associated with the range ID.</td>
</tr>
<tr>
<td>Port-type</td>
<td>Indicates the port type (TCP or UDP)</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.2.1; command introduced.

**Related Commands**

```
app-mon l4port-exclude
```

Configures the L4 port range to exclude from the AppMon operation.

**MIB Objects**

```
alaAppMonEnforcementL4PortRangeTable
   alaAppMonEnforcementL4PortRangeID
   alaAppMonEnforcementL4PortRangeStart
   alaAppMonEnforcementL4PortRangeEnd
   alaAppMonEnforcementL4PortType
   alaAppMonEnforcementL4PortStatus
```
**show app-mon stats**

Displays the number of flow statistics.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `app-mon flow-table enforcement flush` command to clear the counters.

**Examples**

```sh
-> show app-mon stats
Chassis/ Slot       Active Enforcement Matched Flows     Active Used Flows     Total TCP Overflow Flows     Total UDP Overflow Packets
---------+-------------------+----------------+---------------+-----------------+----------------+----------
1/1      8192                  8192             1422            0
2/1      0                   3               0             0
3/1      0                   0               0             0
4/1      0                   0               0             0
Total    8192                  8195             1422            0

-> show app-mon stats
Chassis/ Slot       Active Enforcement Matched Flows     Active Used Flows     Total TCP Overflow Flows
---------+-------------------+----------------+---------------+----------------+
1/1      0                           0              0
Total    0                           0              0
```

**output definitions**

- **Chassis/Slot**: The chassis ID and slot number.
- **Active Enforcement Matched Flows**: Total number of active flows that matched to any active application signature for enforcement feature.
**output definitions (continued)**

<table>
<thead>
<tr>
<th><strong>Active Used Flows</strong></th>
<th>Total number of active flows (including unmatched and enforcement matched) on a given chassis/slot. Each IPv4 flow takes one entry count, while each IPv6 flow takes two entries for Active Used Flows count.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total TCP Overflow Flows</strong></td>
<td>Total number of TCP flows missed to create flow entry in flow table due to hash collision.</td>
</tr>
<tr>
<td><strong>Total UDP Overflow Packets</strong></td>
<td>Cumulative number of UDP packets missed to create flow entry in flow table due to hash collision. <em>This field is displayed only on OmniSwitch 6860.</em></td>
</tr>
</tbody>
</table>

**Release History**

Release 8.2.1; command introduced.

**Related Commands**

```
app-mon flow-table enforcement stats
```

Enable or disable flow table statistics update for enforcement applications.

**MIB Objects**

```
alaAppMonStatisticsTable
  alaAppMonStatsSlotIndex
  alaAppMonTotalEnforcementActiveFlows
  alaAppMonTotalFlowTableInUseFlows
  alaAppMonTCPOverflowFlows
  alaAppMonUDPOverflowPackets
```
**show app-mon aging enforcement**

Displays the aging interval for each application for enforcement feature.

**show app-mon aging enforcement [app-name app_name]**

---

**Syntax Definitions**

*app_name*  
The name of the application. This is a case sensitive string.

---

**Defaults**

By default, the aging time for all applications is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Available</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show app-mon aging enforcement
AppId Application-name TCP Aging-time/UDP Aging-time(minutes)
-----------------------------------------------+-----------------+-------------------------
968  amazon                 6/1
244  facebook               6/1
182  sip                     60/60
183  skype                   6/1
211  tftp                    15/15
503  twitter                6/1
597  viber                   6/1
890  weex                    6/1
1093 whatsapp               6/1
240  youtube                6/1
```
-> show app-mon aging enforcement app-name sip

<table>
<thead>
<tr>
<th>AppId</th>
<th>Application-name</th>
<th>TCP Aging-time/UDP Aging-time (minutes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>182</td>
<td>sip</td>
<td>60/60</td>
</tr>
</tbody>
</table>

**output definitions**

- **AppId**: Identity of the application.
- **Application-name**: Name of the application.
- **TCP Aging-time/UDP Aging-time (minutes)**: Aging time configured for the application.

**Release History**

Release 8.2.1; command introduced.

**Related Commands**

- **app-mon aging enforcement**: Configures the aging time for dynamically learned flows for each application for enforcement feature.

**MIB Objects**

- `alaAppMonEnforcementAgingTimerTable`
- `alaAppMonEnforcementAgingTimerAppName`
- `alaAppMonEnforcementAgingTimerValue`
show app-mon vc-topology

Displays the AppMon virtual chassis topology.

show app-mon vc-topology

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>output</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Displays the topology of the available OmniSwitch 6860 and OmniSwitch 6860E chassis. This also displays the connectivity between the chassis for flow classification.

Examples

-> show app-mon vc-topology

<table>
<thead>
<tr>
<th>Chassis/Slot</th>
<th>Node Type</th>
<th>Designated Chassis/Slot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>OS6860</td>
<td>2/1</td>
</tr>
<tr>
<td>2/1</td>
<td>OS6860E</td>
<td>2/1</td>
</tr>
<tr>
<td>3/1</td>
<td>OS6860E</td>
<td>3/1</td>
</tr>
</tbody>
</table>

output definitions

- **Chassis/Slot**: The chassis ID and slot number.
- **Node Type**: Indicates the switch type.
- **Designated Chassis/Slot**: The chassis and slot of the switch.

Release History

Release 8.2.1; command introduced
Related Commands
N/A

MIB Objects
alaAppMonVCTopologyTable
   alaAppMonVCTopologyChassisIndex
   alaAppMonVCTopologyChassisType
   alaAppMonVCTopologyDesignatedChassisIndex
clear app-mon app-list

Removes all applications from the enforcement or monitor application list.

clear app-mon app-list {monitor| enforcement}

Syntax Definitions

| monitor     | Removes all applications from the monitor application list. |
| enforcement | Removes all applications from the enforcement application list. |

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command does not clear the active application list until the app-mon apply command is used.

Examples

-> clear app-mon app-list enforcement
-> clear app-mon app-list monitor

Release History

Release 8.2.1; command introduced.

Related Commands

app-mon app-list Add or remove applications or application groups to an application list for enforcement or monitoring.

MIB Objects

alaAppMonClearAppList
The OmniSwitch Application Fingerprinting feature attempts to detect and identify remote applications by scanning IP packets and comparing them to pre-defined bit patterns (application signatures). Once an application is identified, Application Fingerprinting collects and stores information about the application flow in a database on the local switch. Additional configurable options for this feature include the ability to apply QoS policy list rules to the identified flow and generating SNMP traps when a signature match occurs.

Using this implementation of Application Fingerprinting, an administrator can obtain more detailed information about protocols running on a specific device or make sure that certain QoS actions are automatically applied wherever an application might be running.

MIB information for the Application Fingerprinting commands is as follows:

Filename: ALCATEL-INI1-APP-FINGERPRINT-MIB.mib
Module: alcatelIN1AppFPMIB

A summary of the available commands is listed here:

- **app-fingerprint admin-state**
- **app-fingerprint port**
- **app-fingerprint signature-file**
- **app-fingerprint reload-signature-file**
- **app-fingerprint trap**
- **show app-fingerprint configuration**
- **show app-fingerprint port**
- **show app-fingerprint app-name**
- **show app-fingerprint app-group**
- **show app-fingerprint database**
- **show app-fingerprint statistics**
**app-fingerprint admin-state**

Enables or disables the Application Fingerprinting process on all Application Fingerprinting ports.

```
app-fingerprint admin-state {enable | disable}
```

**Syntax Definitions**

- **enable**
  - Enables Application Fingerprinting.
- **disable**
  - Disables Application Fingerprinting.

**Defaults**

By default, Application Fingerprinting is enabled for the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When Application Fingerprinting is enabled for the switch, traffic flows on Application Fingerprinting ports are sampled and compared to REGEX application signatures defined in the “app-regex.txt” file located in the `/flash/app-signature` directory on the local switch. This is done to identify the presence of remote applications on a flow-by-flow basis.
- Disabling the administrative status of the Application Fingerprinting feature does not remove the Application Fingerprinting configuration from the switch.

**Examples**

```
-> app-fingerprint admin-state disable
-> app-fingerprint admin-state enable
```

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- **show app-fingerprint configuration**
  - Displays the Application Fingerprinting configuration for the switch.

**MIB Objects**

- `alaAppFPGlobalMIBConfigObjects`
alaAppFPGlobalAdminState
**app-fingerprint port**

Configures a port or link aggregate as an Application Fingerprinting interface. Once the interface is configured and Application Fingerprinting is enabled for the switch, IP packets received on the interface are sampled to determine if they match pre-defined patterns in application signature files that reside on the local switch. When a match occurs, the flow is monitored and/or subject to QoS policy rules.

```plaintext
app-fingerprint {port chassis/slot/port[-port] | linkagg agg_id[-agg_id2]} {monitor-app-group group_name | policy-list-name policy_list | unp-profile}

no app-fingerprint {port chassis/slot/port[-port] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port]` The slot and port number (3/1). Use a hyphen to specify a range of ports.
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of ID numbers (5-10).
- `group_name` The name of an existing signature application group.
- `policy_list` The name of an existing QoS policy list.
- `unp-profile` Apply QoS policy list from UNP to which matching traffic is classified.

**Defaults**

By default, Application Fingerprinting is disabled on all switch ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to disable the Application Fingerprinting service on the specified port or link aggregate.
- Use the `monitor-app-group` parameter to specify a group (profile) that represents a set of application signature files. All of the signature files in the group are checked against the IP packets received on the port. When a packet match is detected, the flow is identified and monitored. No other action is taken.
- Use the `policy-list-name` parameter to associate a QoS policy list with the Application Fingerprinting port. When a packet match is detected, the policy rules in the specified policy list are applied to the matching traffic flow.
Use the `unp-profile` parameter to specify that if traffic received on an Application Fingerprinting interface is classified into a Universal Network Profile (UNP), then the QoS policy list rules associated with that profile are applied to the traffic.

The QoS policy list specified with the `policy-list-name` parameter or assigned to a UNP for Application Fingerprinting traffic, must contain policy rules with the `appfp-group` condition.

The QoS policy list specified with the `policy-list-name` parameter must be configured as an `appfp` list. However, the UNP policy list must be configured as a UNP list.

Application Fingerprinting uses the sFlow mechanism to sample packets. Do not run Application Fingerprinting and other sFlow services on the same port or link aggregate.

**Examples**

-> app-fingerprint port 2/1-5 monitor-app-group my-p2p

-> app-fingerprint linkagg 10 policy-list-name list1

-> app-fingerprint port 1/11 unp

-> no app-fingerprint port 2/1-5

-> no app-fingerprint linkagg 10

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

`show app-fingerprint port` Displays the Application Fingerprinting port configuration.

**MIB Objects**

`alaAppFPPortTable`

`alaAppFPPort`  
`alaAppFPGroupNameOrPolicyList`

`alaAppFPPortOperationMode`

`alaAppFPPortStatus`

`alaAppFPPortRowStatus`
**app-fingerprint signature-file**

Specifies the name of the Application Fingerprinting signature file. This file contains the REGEX signatures that are used to identify applications accessing the network on Application Fingerprinting ports.

**Syntax Definitions**

`filename` The name of an existing REGEX application signature file.

**Defaults**

By default, the “app-regex.txt” file is used.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command is only required to use a REGEX signature file that has a filename that is different from the default “app-regex.txt” name.
- The signature file must reside in the `/flash/app-signature` directory on the local switch.
- After specifying the signature filename to use, upload the signature file into the switch memory using the `app-fingerprint reload-signature-file` command.

**Examples**

`-> app-fingerprint signature-file app2_regex.txt`

**Release History**

Release 7.3.2; command was introduced.
Related Commands

app-fingerprint reload-signature-file  Reloads the contents of the active application signature file into the switch memory.

MIB Objects

alaAppFPGlobalMIBConfigObjects
alaAppFPGlobalSignatureFile
**app-fingerprint reload-signature-file**

Reloads the contents of the active application signature file into the switch memory. Use this command after making any changes to the current signature file.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command reloads the application signature file that was previously applied to the switch. This may be the default “app-regex.txt” file or another signature file that was applied through the **app-fingerprint signature-file** command.

- A switch reboot is *not* required after the signature file is reloaded.

**Examples**

```
-> app-fingerprint reload-signature-file
```

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- **app-fingerprint signature-file** Specifies a different signature file to use for Application Fingerprinting.

**MIB Objects**

- `alaAppFPGlobalMIBConfigObjects`
- `alaAppFPGlobalReloadSignatureFile`
**app-fingerprint trap**

Enables or disables trap generation for the Application Fingerprinting feature.

`app-fingerprint trap {enable | disable}`

---

**Syntax Definitions**

- **enable**: Enables Application Fingerprinting traps.
- **disable**: Disables Application Fingerprinting traps.

---

**Defaults**

By default, traps are disabled for this feature.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

A trap is generated when a traffic flow matches an application signature.

---

**Examples**

- `-> app-fingerprint trap enable`
- `-> app-fingerprint trap disable`

---

**Release History**

Release 7.3.2; command was introduced.

---

**Related Commands**

- `show app-fingerprint configuration`: Displays the Application Fingerprinting status and configuration for the switch.

---

**MIB Objects**

- `alaAppFPGlobalMIBConfigObjects`
- `alaAppFPGlobalTrapConfig`
show app-fingerprint configuration

Displays the Application Fingerprinting status and configuration information for the switch.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin-state</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Signature File</td>
<td>app-regex.txt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show app-fingerprint configuration

Admin-state: Enabled,
SNMP Trap: Disabled,
Signature File: app-regex.txt

output definitions

| Admin-state | The administrative status of Application Fingerprinting for the switch (Enabled or Disabled). Configured through the app-fingerprint admin-state command. |
| SNMP Trap | The status of SNMP trap generation for the switch (Enabled or Disabled). Configured through the app-fingerprint trap command. |
| Signature File | The name of the text file that contains the REGEX application signatures used to identify traffic flows. This file resides in the /flash/app-signature directory on the switch. Configured through the app-fingerprint signature-file and app-fingerprint reload-signature-file commands. |
Release History

Release 7.3.2; command was introduced.

Related Commands

show app-fingerprint port  Displays the Application Fingerprinting port configuration.

MIB Objects

alaAppFPGlobalMIBConfigObjects
  alaAppFPGlobalAdminState
  alaAppFPGlobalSignatureFile
  alaAppFPGlobalReloadSignatureFile
  alaAppFPGlobalTrapConfig
show app-fingerprint port

Displays the Application Fingerprinting port configuration for the switch.

show app-fingerprint [port chassis/slot/port | linkagg agg_id]

Syntax Definitions

chassis
   The chassis identifier.

slot/port|port
   The slot and port number (3/1).

agg_id
   The link aggregate ID number.

Defaults

By default, the configuration for all Application Fingerprinting ports is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>V72/C32</td>
<td>X48C6/T48C6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the port and linkagg parameters to display information for a specific port or link aggregate.

Examples

-> show app-fingerprint port
Legend: * = Port or App-Group is invalid

<table>
<thead>
<tr>
<th>Port</th>
<th>Operation Mode</th>
<th>App-group/Policy-list</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2/1</td>
<td>Monitoring</td>
<td>Testing13</td>
</tr>
<tr>
<td>1/2/1</td>
<td>QoS</td>
<td>list1</td>
</tr>
<tr>
<td>1/2/1</td>
<td>QoS</td>
<td>list2</td>
</tr>
</tbody>
</table>

-> show app-fingerprint linkagg
Legend: * = Port or App-Group is invalid

<table>
<thead>
<tr>
<th>Port</th>
<th>Operation Mode</th>
<th>App-group/Policy-list</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/100</td>
<td>Monitoring</td>
<td>Testing16</td>
</tr>
<tr>
<td>0/100</td>
<td>QoS</td>
<td>list3</td>
</tr>
<tr>
<td>0/100</td>
<td>QoS</td>
<td>list4</td>
</tr>
</tbody>
</table>
**output definitions**

| Port | The slot/port or link aggregate ID of the Application Fingerprinting interface. A “0” slot number indicates that the interface is a link aggregate. |
| Operation Mode | The Application Fingerprinting mode (Monitoring, QoS, or UNP) in which the port is operating. |
| App-group/Policy-list | The name of the group of application signatures or the QoS policy list that is applied to the traffic flows on the port. |

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- `show app-fingerprint port` Displays the Application Fingerprinting interface configuration.
- `show app-fingerprint configuration` Displays the Application Fingerprinting status and configuration for the switch.

**MIB Objects**

- `alaAppFPPortTable`
  - `alaAppFPPort`
  - `alaAppFPGroupNameOrPolicyList`
  - `alaAppFPPortOperationMode`
  - `alaAppFPPortStatus`
  - `alaAppFPPortRowStatus`
show app-fingerprint app-name

Displays the REGEX application signature configuration for the switch. When the switch samples Application Fingerprinting ports, the traffic flow patterns on these ports are compared against the REGEX signatures specified in the “app-regex.txt” file. When a match occurs, the traffic flow is classified and monitored. In addition, QoS policies can be applied to these flows based on a specific match to an application signature group.

show app-fingerprint app-name [app_name]

Syntax Definitions

app_name

The name of an existing application signature.

Defaults

By default, all application signatures are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Application signatures are defined in the “app-regex.txt” file that resides in the /flash/app-signature directory on the switch. A default version of this file is available, but the file is user-configurable and new files can also be created.

- Application signatures can also be combined into an application group. This type of group is then assigned to one or more Application Fingerprinting ports. All the application signatures that are members of the assigned group are then applied to traffic flows on that same port.

- Use the app_name parameter to display information for a specific application signature.

Examples

-> show app-fingerprint app-name
App Name: ciscovpn
  Description: VPN client software to a Cisco VPN server
  REGEX Signature: \\x01\xf4\\x01\xf4

App Name: citrix
  Description: Citrix ICA - proprietary remote desktop application
  REGEX Signature: \x32\x26\x85\x92\x58

App Name: dhcp
  Description: Dynamic Host Configuration Protocol
show app-fingerprint app-name

App Name: citrix
Description: Citrix ICA - proprietary remote desktop application
REGEX Signature: \x32\x26\x85\x92\x58

<table>
<thead>
<tr>
<th>output definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>App-name</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>REGEX signature</td>
</tr>
</tbody>
</table>

Release History
Release 7.3.2; command was introduced.

Related Commands
- show app-fingerprint app-group
  Displays the application group configuration.
- show app-fingerprint configuration
  Displays the Application Fingerprinting status and configuration.

MIB Objects
alaAppFPAppGrpNameTable
alaAppFPGrpAppName
show app-fingerprint app-group

Displays the Application Fingerprinting application group configuration for the switch. An application group contains a user-configured list of REGEX application signatures that are represented by the group name. The group name is then assigned to Application Fingerprinting ports or link aggregates.

**show app-fingerprint app-group [group_name]**

**Syntax Definitions**

*group_name* The name of an existing application group.

**Defaults**

By default, all application groups are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Application groups are defined in the “app-regex.txt” file that is located in the `/flash/app-signature` directory on the switch. A default version of this file is available, but the file is user-configurable and new files can also be created.

- Use the *group_name* parameter to display information for a specific application group.

**Examples**

-> show app-fingerprint app-group

App Group: chatting
   App names: jabber

App Group: mail
   App names: smtp

App Group: network
   App names: bgp dhcp rtsp smb

App Group: p2p
   App names: hotline

App Group: remote_access
   App names: ciscovpn citrix rdp ssh vnc
App Group: voip
  App names: h323 sip
-> show app-fingerprint app-group network

App Group: network
  App names: bgp dhcp rtsp smb

**output definitions**

<table>
<thead>
<tr>
<th>App-Group</th>
<th>The name of the application group file.</th>
</tr>
</thead>
<tbody>
<tr>
<td>App names</td>
<td>The names of the application signature files that belong to this group.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- **show app-fingerprint app-name**
  Displays the contents of the REGEX application signatures that are stored in the “app-regex.txt” file on the switch.

- **show app-fingerprint configuration**
  Displays the Application Fingerprinting status and configuration.

**MIB Objects**

- ```alaAppFPAppGrpNameTable```
- ```alaAppFPAppGroupName```
- ```alaAppFPGrpAppName```
show app-fingerprint database

Displays Application Fingerprinting database entries. When a match occurs between an IP traffic flow and a REGEX application signature, a multi-tuple classifier and the name of the matching application group and signature are stored in a local switch database to identify and track the application associated with the flow.

```
show app-fingerprint database [port chassis/slot/port | linkagg agg_id] [detail]
```

Syntax Definitions

- `chassis`: The chassis identifier.
- `slot/port`: The slot and the port number (3/1).
- `agg_id`: The link aggregate ID number.
- `detail`: Displays additional information about the classified traffic flow.

Defaults

By default, all application flow database entries are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `port` and `linkagg` parameters to display information for a specific port or link aggregate.
- The following multi-tuple classifier is used to identify an application traffic flow:
  - Ingress Port
  - Dest MAC
  - Src MAC
  - VLAN
  - Dest IP
  - Src IP
  - Dest Port
  - Src Port
- Each database entry is subject to a 15 minute aging period. If the database fills up, older entries are aged out before the 15 minute limit (fast aging). However, fast aging is not applied to database entries associated with QoS. In this case, the QoS is removed after the regular 15 minute aging time period expires.
When a database entry is removed due to regular aging or fast aging conditions, any corresponding QoS is also removed for that flow.

**Examples**

```
-> show app-fingerprint database
```

<table>
<thead>
<tr>
<th>Port</th>
<th>App-Group/Name</th>
<th>SRC MAC</th>
<th>VLAN</th>
<th>SRC IP/Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1/2</td>
<td>P2P/aim</td>
<td>00:00:22:33:44:55</td>
<td>20</td>
<td>2.3.4.4/200</td>
</tr>
<tr>
<td>0/1/2</td>
<td>P2P/ares</td>
<td>00:00:22:33:44:55</td>
<td>20</td>
<td>2.3.4.4/200</td>
</tr>
<tr>
<td>0/1/2</td>
<td>Mail/smtp</td>
<td>00:00:22:33:44:55</td>
<td>20</td>
<td>2.3.4.4/100</td>
</tr>
</tbody>
</table>

```
-> show app-fingerprint database detail
```

Port 1/2/1:

- **App-Group/Name**: Testing2/App_4
  - SRC-DST MAC: 00:00:00:04:01 - 00:e0:b1:e6:f9:b5
  - VLAN: 20
  - SRC IP/PORT: 20.20.20.21/65
  - DST IP/PORT: 10.10.10.11/55

- **App-Group/Name**: Testing2/App_5
  - SRC-DST MAC: 00:00:00:04:02 - 00:e0:b1:e6:f9:b5
  - VLAN: 20
  - SRC IP/PORT: 20.20.20.21/64
  - DST IP/PORT: 10.10.10.11/54

- **App-Group/Name**: Testing2/App_6
  - SRC-DST MAC: 00:00:00:04:03 - 00:e0:b1:e6:f9:b5
  - VLAN: 20
  - SRC IP/PORT: 20.20.20.21/66
  - DST IP/PORT: 10.10.10.11/56

Port 2/3/23:

- **App-Group/Name**: Testing1/App_1
  - SRC-DST MAC: 00:00:00:03:01 - 00:e0:b1:e6:f9:b5
  - VLAN: 10
  - SRC IP/PORT: 10.10.10.11/115
  - DST IP/PORT: 20.20.20.21/137

- **App-Group/Name**: Testing1/App_2
  - SRC-DST MAC: 00:00:00:03:02 - 00:e0:b1:e6:f9:b5
  - VLAN: 10
  - SRC IP/PORT: 10.10.10.11/114
  - DST IP/PORT: 20.20.20.21/138

**output definitions**

- **Port**: The slot/port or link aggregate ID of the AFP interface on which the flow was classified. A “0” slot number indicates a link aggregate.
- **App-Group/Name**: The name of the application group and signature that matched the flow.
- **SRC MAC**: The source MAC address of the flow.
- **VLAN**: The VLAN on which the flow is learned and forwarded.
- **SRC IP/PORT**: The source IP network address and port.
Application Fingerprinting Commands

App-Group/Name: Testing1/App_3
SRC-DST MAC: 00:00:00:00:03:03 - 00:e0:b1:e6:f9:b5,
VLAN: 10,
SRC IP/PORT: 10.10.10.11/113,
DST IP/PORT: 20.20.20.21/135

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The slot and port number on which the flow was classified.</td>
</tr>
<tr>
<td>App-Group/Name</td>
<td>The name of the application group and signature that matched the flow.</td>
</tr>
<tr>
<td>SRC-DST MAC</td>
<td>The source and destination MAC addresses of the flow.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN on which the flow is learned and forwarded.</td>
</tr>
<tr>
<td>SRC IP/Port</td>
<td>The source IP network address and port.</td>
</tr>
<tr>
<td>DST IP/Port</td>
<td>The destination IP network address and port.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command was introduced.

Related Commands

- **show app-fingerprint app-group**
  - Displays the application group configuration.
- **show app-fingerprint configuration**
  - Displays the Application Fingerprinting status and configuration.

MIB Objects

- `alaAppFPDatabaseTable`
  - `alaAppFPDbPort`
  - `alaAppFPDbAppGroupName`
  - `alaAppFPDbAppName`
  - `alaAppFPDbSrcMacAddr`
  - `alaAppFPDbVlanId`
  - `alaAppFPDbSrcIpAddrType`
  - `alaAppFPDbSrcIpAddr`
  - `alaAppFPDbSrcPort`
  - `alaAppFPDbDstIpAddrType`
  - `alaAppFPDbDstIpAddr`
  - `alaAppFPDbDstPort`
  - `alaAppFPDbDstMacAddr`
**show app-fingerprint statistics**

Displays statistics for each application flow on an Application Fingerprinting ingress port.

**show app-fingerprint statistics [port chassis/slot/port | linkagg agg_id]**

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot and the port number (3/1).
- **agg_id**: The link aggregate ID number.

### Defaults

By default, statistics are displayed for all application flows.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.
- Statistics displayed with this command include total number of packets matched, the number of unmatched packets, and the packets matched for each application signature.

### Examples

```
-> show app-fingerprint statistics
  Port | Group/App name | Last 1 hour | Last 1 day |
  1/2/1 | Testing2/App_4   | 19976        | 19976      |
  1/2/1 | Testing2/App_5   | 20000        | 20000      |
  1/2/1 | Testing2/App_6   | 20000        | 20000      |
  2/3/23 | Testing1/App_1   | 19975        | 19975      |
  2/3/23 | Testing1/App_2   | 20000        | 20000      |
  2/3/23 | Testing1/App_3   | 20000        | 20000      |
```

### Release History

Release 7.3.2; command introduced.
Related Commands

show app-fingerprint port  Displays the Application Fingerprinting interface configuration.

MIB Objects

alaAppFPStatsTable
alaAppFPStatsPort
alaAppFPStatsGroupName
alaAppFPStatsAppName
alaAppFPPTotalMatchedLast1Hour
alaAppFPPTotalMatchedLast1Day
The OmniSwitch implementation of Fibre Channel over Ethernet (FCoE) Initiation Protocol (FIP) snooping supports the FCoE technology used to tunnel Fibre Channel (FC) frames within Ethernet MAC frames. When the FCoE and FIP snooping functionality is enabled, the OmniSwitch serves as an FCoE transit switch. In this role, the OmniSwitch implementation of Data Center Bridging (DCB) is also used to provide the lossless Ethernet network required to support FCoE.

This implementation of FIP snooping ensures the security of the FCoE network and maintains a virtual point-to-point network connection between FCoE Nodes (ENodes) and FCoE Forwarder (FCF) devices. In addition, FIP snooping is also required to support OmniSwitch FCoE/FC gateway functionality that allows the switch to provide FCoE forwarding services between an FCoE network and a native FC storage area network (SAN).

- An OmniSwitch FCoE transit switch is placed between ENodes (servers or other bridges) and an FCF or an OmniSwitch FCoE/FC gateway to extend the reach of the FCoE network without extending the physical FC connections.
- An OmniSwitch FCoE/FC gateway runs FIP snooping on the 10G Ethernet FCoE ports that connect to an FCoE network. On the same switch, FC ports connect to native FC switches or nodes. Traffic is transmitted between the FCoE network and the FC SAN through the gateway switch.

This chapter provides information about configuring FCoE and FIP global and port parameters through the Command Line Interface (CLI). See Chapter 44, “FCoE/FC Gateway Commands,” for more information about configuring OmniSwitch FCoE/FC gateway functionality.

MIB information for the FCoE and FIP snooping commands is as follows:

- **Filename:** ALCATEL-IND1-FIPS-MIB.mib
- **Module:** alcatelIND1FipsMIB

The FCoE and FIP Snooping commands are listed here:

<table>
<thead>
<tr>
<th>Global commands</th>
<th>VLAN and Port commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcoe fip-snooping</td>
<td>fcoe fcoe vlan</td>
</tr>
<tr>
<td>fcoe address-mode</td>
<td>fcoe fcoe fcf mac</td>
</tr>
<tr>
<td>fcoe priority</td>
<td>fcoe fcoe fc-map</td>
</tr>
<tr>
<td>fcoe priority-protection</td>
<td>fcoe fcoe discovery-advertisement</td>
</tr>
<tr>
<td>fcoe priority-protection action</td>
<td>fcoe fcoe role</td>
</tr>
<tr>
<td>fcoe filtering-resource trap-threshold</td>
<td></td>
</tr>
<tr>
<td>fcoe house-keeping-time-period</td>
<td></td>
</tr>
</tbody>
</table>
### FIP Snooping Commands

| Show commands          | show fcoe
|                       | show fcoe ports
|                       | show fcoe sessions
|                       | show fcoe enode
|                       | show fcoe fcf
|                       | show fcoe fc-map
|                       | show fcoe discovery-advertisement
| Statistics commands   | show fcoe statistics
|                       | clear fcoe statistics |
**fcoe fip-snooping**

Enables or disables Fibre Channel Initiation Protocol (FIP) snooping on the switch. FIP Snooping is enabled to allow the OmniSwitch to serve as an FCoE transit switch.

`fcoe fip-snooping admin-state {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>Enables FIP Snooping.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable</td>
<td>Disables FIP Snooping.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When FIP Snooping is enabled, traffic with an Ethertype of FCoE is dropped on all switch VLANs and ports that are not configured as FCoE VLANs and ports.

**Examples**

- `-> fcoe fip-snooping admin-state enable`
- `-> fcoe fip-snooping admin-state disable`

**Release History**

Release 7.3.2; command was introduced.
Related Commands

show fcoe  Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

alaFipsConfig
  alaFipsConfigFIPSAdmin
fcoe address-mode

Configures the FCoE addressing mode. This mode determines whether a server-provided MAC address (SPMA) or a fabric-provided MAC address (FPMA) is assigned to virtual FCoE entities.

fcoe address-mode {spma | fpma}

Syntax Definitions

spma                     Selects the SPMA address mode.
fpma                     Selects the FPMA address mode.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>spma</td>
<td>fpma</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>spma</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>fpma</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The FCoE Node (ENode) and the FCoE Forwarder (FCF) must use the same addressing mode to establish virtual links between the ENode and FCF. Configure the global OmniSwitch addressing mode to match the mode used by the ENode and FCF.

- When the FPMA mode is active, a MAC address is assigned by an FCF to a single ENode MAC. This MAC address is not assigned to any other ENode MAC in the same VLAN.

- When the SPMA mode is active, MAC addresses are assigned by the ENode server.

- To change the addressing mode selection, disable FIP Snooping for the switch then make the change and enable FIP Snooping again.

Examples

- fcoe address-mode spma
- fcoe address-mode fpma

Release History

Release 7.3.2; command was introduced.
Related Commands

- **fcoe fip-snooping**: Enables or disables FIP Snooping on the switch
- **show fcoe**: Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

- **alaFipsConfig**
  - **alaFipsConfigAddressMode**
**fcoe priority**

Configures up to two global priority values that are designated as lossless for FCoE traffic.

```
fcoe priority {priority} [priority]
```

---

**Syntax Definitions**

| priority | A priority value between 0–7. |
---|---|

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>3</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command overwrites the existing FCoE priority values used by the switch.
- If two priority values are configured but there is a need to change only one of the values, both priority values must be specified with this command. For example, if the current priority is set to 2 and 5, to change priority 2 to 3, specify both 3 and 5 as the priority values.
- Specify a priority value of 3 to set the priority back to the default value.
- The FCoE priority values are used when FCoE priority protection is enabled for the switch.
- In addition to enabling priority protection, a lossless DCB FCoE profile with the same FCoE priority values must be assigned to the FCoE interfaces.

**Examples**

```
-> fcoe priority 2 5
-> fcoe priority 3 5
-> fcoe priority 3
```

**Release History**

Release 7.3.2; command was introduced.
Related Commands

- **fcoe priority-protection**
  - Configures the status of priority protection for the switch.

- **fcoe priority-protection action**
  - Configures the action taken when traffic is not FCoE or FIP.

- **fcoe fip-snooping**
  - Enables or disables FIP Snooping on the switch

- **show fcoe**
  - Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

- alaFipsConfig
  - alaFipsConfigPriorityOne
  - alaFipsConfigPriorityTwo
**fcoe priority-protection**

Enables or disables priority protection.

```
fcoe priority-protection {enable | disable}
```

### Syntax Definitions

- **enable**: Enables priority protection for the switch.
- **disable**: Disables priority protection for the switch.

### Defaults

By default, priority protection is disabled for the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When priority protection is enabled, only FCoE and FIP traffic that matches the FCoE lossless priority values is allowed. All other traffic is either marked or dropped, based on the priority protection action configured for the switch.
- This command applies only to the priority value that is specified using the `fcoe priority` command.
- The FCoE priority value is advertised to FCoE-enabled hosts using the Data Center Bridging Exchange (DCBx) protocol.

### Examples

```
-> fcoe priority-protection enable
-> fcoe priority-protection disable
```

### Release History

Release 7.3.2; command was introduced.
Related Commands

- `fcoe priority` Configures the lossless priority values for the switch.
- `fcoe priority-protection action` Determines whether non-FCoE and non-FIP traffic is dropped or marked with a lower priority value.
- `fcoe fip-snooping` Enables or disables FIP Snooping on the switch
- `show fcoe` Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

alaFipsConfig
  alaFipsConfigPrioProtection


fcoe priority-protection action

Specifies whether non-FCoE and non-FIP traffic is dropped or marked with a lower priority value. This action is only valid when FCoE priority protection is enabled for the switch.

fcoe priority-protection action {drop | remark priority}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>All non-FCoE and non-FIP traffic is dropped.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the priority value to use for remarking non-FCoE and non-FIP traffic.</td>
</tr>
</tbody>
</table>

Defaults

By default, non-FCoE and non-FIP traffic is dropped when priority protection is enabled for the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When priority protection is enabled, only FCoE traffic that matches the protected priority values is allowed in the priority queues. All other traffic is either re-marked or dropped, based on the priority protection action configured for the switch.
- If the re-mark action is configured, traffic is marked with the specified priority value and forwarded on the switch.

Examples

-> fcoe priority-protection action drop
-> fcoe priority-protection action remark 0

Release History

Release 7.3.2; command was introduced.
Related Commands

- **fcoe priority**
  Configures the lossless priority values for the switch.

- **fcoe priority-protection**
  Configures the status of priority protection for the switch.

- **fcoe fip-snooping**
  Enables or disables FIP Snooping on the switch.

- **show fcoe**
  Displays the FCoE and FIP snooping status and configuration for the switch.

MIB Objects

**alaFipsConfig**

- **alaFipsConfigPriorityProtectionAction**
**fcoe filtering-resource trap-threshold**

Configures the percentage of filtering resources used as a trap threshold value. When this percentage is reached, a trap is generated by the switch.

`fcoe filtering-resource trap-threshold percentage`

**Syntax Definitions**

`percentage` The percentage of filtering resources used.

**Defaults**

By default, the filtering resource trap threshold percentage is set to 80%.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To disable the generation of filtering resource traps, set the trap threshold value to “0”.

**Examples**

`-> fcoe filtering-resource trap-threshold 50`
`-> fcoe filtering-resource trap-threshold 0`

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- `show fcoe` Displays the FCoE and FIP snooping status and configuration for the switch.

**MIB Objects**

Notifications (Traps)

- `alaFipsResourceThresholdReached`
- `alaFipsFilterResourceUsage`
**fcoe house-keeping-time-period**

Configures the amount of time the FCoE switch waits to receive keep alive messages from the ENode and FCF for a given FCoE session. When this time expires and no keep alive messages were received for any entity of the session, the session information is removed.

**fcoe house-keeping-time-period** *seconds*

---

**Syntax Definitions**

*seconds* The keep alive wait time, in seconds.

**Defaults**

By default, the housekeeping timer is set to 300 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To disable the housekeeping timer, set the timer value to “0”

**Examples**

- `-> fcoe house-keeping-time-period 120`
- `-> fcoe house-keeping-time-period 0`

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- `show fcoe` Displays the FCoE and FIP snooping status and configuration for the switch.

**MIB Objects**

- `alaFipsConfig`
  - `alaFipsConfigHouseKeepingTimePeriod`
**fcoe vlan**

Configures an FCoE VLAN. This type of VLAN is used to deploy the OmniSwitch implementation of FIP snooping.

```
fcoe vlan vlan_id [admin-state {enable | disable}] [name description]
no fcoe vlan vlan_id
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan_id</code></td>
<td>A numeric value that uniquely identifies an individual FCoE VLAN. The valid ID range is 2–4094.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables the FCoE VLAN administrative status.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disables the FCoE VLAN administrative status.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>An alphanumeric string. Optional name description for the VLAN ID. Enclose the description in double quotes if it contains more than one word with a space in between.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td><code>enable</code></td>
</tr>
<tr>
<td><code>description</code></td>
<td><code>VLAN ID</code></td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

- Use the `no` form of this command to remove a FCoE VLAN from the switch configuration. All VLAN ports are detached before the VLAN is removed.
- Specify a VLAN ID that does not exist in the switch configuration, or the ID of a dynamically created MVRP VLAN.
- Only 802.1q-tagged FCoE ports and link aggregates can be members of FCoE VLANs.
- Configuring a FCoE VLAN as a default VLAN for a port or link aggregate is not allowed. All port associations are created by tagging FCoE ports with the FCoE VLAN ID.
- Configuring default VLAN 1 as an FCoE VLAN is not allowed.
The following features are not supported on FCoE VLANs:
- IGMP Snooping
- IP interface
- HA VLANs
- SVLAN and CVLAN
- Shortest Path Bridging (SPB)
- UDP Relay, DHCP Snooping
- Universal Network Profile (UNP)

An OmniSwitch FCoE transit switch operates between an FCoE Node (ENode) and a FCoE Forwarder (FCF). Manual configuration of the FCoE VLAN is required along the transit switch path. However, the ENode and FCF may invoke FIP VLAN discovery to discover the FCoE VLANs within the transit path. If not, manual configuration of the FCoE VLANs may also be required on the appropriate ENodes and FCFs.

**Examples**

```
-> fcoe vlan 100
-> no fcoe vlan 100
-> fcoe vlan 100 admin-state enable name fcoe-vlan1
-> fcoe vlan 100 admin-state enable
```

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

- **fcoe fcf mac**
  Configures a static Fibre Channel Forwarder (FCF) MAC address for the specified FCoE VLAN.

- **fcoe fip-snooping**
  Enables or disables FIP Snooping on the switch

- **show vlan**
  Displays the VLAN configuration for the switch.

**MIB Objects**

<table>
<thead>
<tr>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaFipsVlanTable</td>
</tr>
<tr>
<td>alaFipsVlanId</td>
</tr>
<tr>
<td>alaFipsVlanFCMap</td>
</tr>
<tr>
<td>alaFipsVlanRowStatus</td>
</tr>
</tbody>
</table>
**fcoe fcf mac**

Configures a static Fibre Channel Forwarder (FCF) MAC address for the specified FCoE VLAN. Virtual Fibre Channel (FC) links that traverse the lossless Ethernet network send FCoE frames to and from the FCF MAC address.

```
fcoe fcf mac mac_address vlan vlan_id
no fcoe fcf mac_address vlan vlan_id
```

---

**Syntax Definitions**

- **mac_address**: Enter the FCF MAC Address (for example, 00:00:39:59:f1:0c).
- **vlan_id**: An existing FCoE VLAN ID. The valid ID range is 2–4094.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the no form of this command to remove the FCF MAC address from the specified FCoE VLAN.
- The FCoE VLAN ID must already exist in the switch configuration.

---

**Examples**

```
-> fcoe fcf mac 30:10:94:01:00:00 vlan 100
-> no fcoe fcf 30:10:94:01:00:00
```

---

**Release History**

Release 7.3.2; command introduced.
Related Commands

- **fcoe vlan**: Configures an FCoE VLAN for the switch.
- **fcoe fip-snooping**: Enables or disables FIP Snooping on the switch.
- **show vlan**: Displays the VLAN configuration for the switch.

MIB Objects

- **alaFipsVlanTable**
  - **alaFipsVlanId**
  - **alaFipsVlanFCMap**
**fcoe fc-map**

Configures a static Fibre Channel Mapped Address Prefix (FC-MAP) for the specified FCoE VLAN. The FC-MAP is a 24-bit value used by the Fibre Channel Forwarder (FCF) to identify an individual fabric.

```
fcoe fc-map prefix vlan vlan_id
no fcoe fc-map prefix vlan vlan_id
```

### Syntax Definitions

- **prefix**
  - Enter the FC-MAP prefix value. The valid range is 0EFC00–0EFCFF.

- **vlan_id**
  - An existing FCoE VLAN ID. The valid ID range is 2–4094.

### Defaults

By default, the FC-MAP is set to 0E:FC:00.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- On an OmniSwitch 6900, use the `no` form of this command to set the FC-MAP back to the default value (0E:FC:00) for the specified FCoE VLAN.

- The FCoE VLAN ID must already exist in the switch configuration.

- The configured FC-MAP value assigned to an FCoE VLAN must match the FC-MAP value used by the FCF device. FCF advertisement packets that contain a different FC-MAP are not processed by the switch.

- When the FCoE address mode is set to Fabric-Provided MAC Address (FPMA), the FCF uses the FC-MAP value (upper 24 bits) combined with an FCID value (lower 24 bits) to generate a unique MAC address to identify an ENode VN_Port for FCoE transactions.

### Examples

```
-> fcoe fc-map 0E:FC:04 vlan 30
-> no fcoe fc-map 0E:FC:04 vlan 30
```

### Release History

Release 7.3.2; command introduced.
Related Commands

- **fcoe vlan**: Configures an FCoE VLAN for the switch.
- **fcoe fip-snooping**: Enables or disables FIP Snooping on the switch.
- **show vlan**: Displays the VLAN configuration for the switch.

MIB Objects

- **alaFipsVlanTable**
  - **alaFipsVlanId**
  - **alaFipsVlanFCMap**

---

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 43-20
**fcoe discovery-advertisement**

Configures FIP discovery advertisement message parameters for the specified FCoE VLAN. These parameter values are advertised in both unicast and multicast advertisements.

```
fcoe discovery-advertisement vlan vlan_id[-vlan_id2] [a-bit {enable | disable}] [fka-adv-period adv_seconds] [priority priority] [uds-retries retries]
```

**Syntax Definitions**

- `vlan_id[-vlan_id2]` An existing FCoE VLAN ID. Use a hyphen to specify a range of FCoE VLAN IDs (10-25).
- `enable` Enables the available-for-login bit (A-bit) in the discovery advertisement message to indicate that the switch can accept fabric logins from ENodes.
- `disable` Disables the A-bit in the discovery advertisement message to indicate that the switch cannot accept fabric logins from ENodes.
- `adv_seconds` The discovery advertisement transmission interval and the number of FIP ENode keep alive packets expected. The valid range is 1–90 seconds.
- `priority` The priority value assigned to the switch, indicated in the priority descriptor of the discovery advertisement message. The valid range is 0–255 (0 = highest priority, 255 = lowest priority).
- `retries` The number of times a unicast discovery solicitation is transmitted after a port on which an FCF MAC was learned goes down. The valid range is 0–10.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>a-bit enable</td>
<td>enable</td>
</tr>
<tr>
<td>fka-adv-period adv_seconds</td>
<td>8</td>
</tr>
<tr>
<td>priority priority</td>
<td>128</td>
</tr>
<tr>
<td>uds-retries retries</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 43-21
Usage Guidelines

- When the A-bit parameter is disabled, the switch will not process any new logins for the FCoE VLAN. However, there is no impact on existing VN_Port sessions, which are allowed to continue.

- Transmitting unicast discovery solicitations helps to find out if the same FCF is reachable on some other port of the same FCoE VLAN.

Examples

-> fcoe discovery-advertisement vlan 100 priority 10
-> fcoe discovery-advertisement uds-retries 3
-> no fcoe discovery-advertisement vlan 100

Release History

Release 7.3.3; command introduced.

Related Commands

show fcoe discovery-advertisement Displays the discovery advertisement parameter values for the specified VLANs.

MIB Objects

alaFipsDiscAdvtTable
  alaFipsDiscAdvtVlanId
  alaFipsDiscAdvtAbit,
  alaFipsDiscAdvtFkaAdvPeriod,
  alaFipsDiscAdvtPriority,
  alaFipsDiscAdvtUdsRetries,
  alaFipsDiscAdvtRowStatus
**fcoe role**

Configures the specified port or link aggregate as an FCoE interface and defines the role of the interface in the FCoE network.

```plaintext
fcoe {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} role {edge | enode-only | fcf-only | mixed | trusted | ve}

no fcoe {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- `chassis` The chassis identifier when running in virtual chassis mode.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). FCoE is only supported on 10G or faster ports.
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `edge` Port connects directly to an ENode for transmission of FCoE and FIP frames from the ENode to the FCF.
- `enode-only` Link between FCoE switches that carries traffic from ENode to FCF.
- `fcf-only` Link between FCoE switches that carries traffic from FCF to ENode.
- `mixed` Link between FCoE switches that carries traffic in both directions (from FCF to ENode or from ENode to FCF).
- `trusted` Trust the FCoE Edge port; traffic on this port is not filtered by FIP ACLs. This port role type is typically assigned to the switch FCoE port that connects to an Ethernet port on the FCF.
- `ve` Configures port as a virtual expansion port (VE_Port) that is associated with an E2E-tunnel session. A VE_Port emulates an E_Port in an FCoE network, providing connectivity between FC switches. VE_Ports discover FCFs.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 43-23
**Usage Guidelines**

- Use the `no` form of this command to revert the FCoE port back to a regular switch port. Before doing so, however, delete any associations the port may have with an FCoE VLAN.

- To change the role of an FCoE port, first remove the FCoE configuration from the port, then configure FCoE and the new role again for that same port.

- FCoE is only supported on 10G or faster ports that are associated with an FCoE lossless DCB profile. In addition, DCBX must be enabled on the port with both PFC and ETS in an active state (either forced or negotiated via DCBX). The DCB configuration is done separately using QoS port and profile commands.

- The maximum frame size for an FCoE port must be at least 2500 bytes to accommodate FCoE encapsulated frames, which are larger than the standard Ethernet frame size. In addition, make sure the FCoE port frame size is configured the same end-to-end.

- When configuring a link aggregate as an FCoE port, make sure the link aggregate ID number already exists in the switch configuration. Ports already configured as FCoE ports cannot be added to a link aggregate.

- FCoE ports must be manually assigned to a default VLAN and then tagged with the FCoE VLAN that will carry the FCoE and FIP frames on that port.

- The following features are not supported on FCoE ports:
  - Learned Port Security (LPS)
  - Port Mirroring and Remote Port Mirroring
  - Shortest Path Bridging (SPB)

- Enabling FCoE on a Universal Network Profile (UNP) port is only supported to allow UNP dynamic assignment of a default VLAN for an FCoE port. Manual tagging of the FCoE UNP port with FCoE VLAN IDs is still required.

- FCoE VLANs may be dynamically learned through the transmission of MVRP join PDU, but any port associations with that VLAN must be manually configured.

- Assigning FCoE interfaces to different FCoE VLANs provides a method for configuring multiple FC fabrics through the same FCoE switch.

**Examples**

- `fcoe port 1/1 role edge`
- `fcoe port 1/1/1 role edge`
- `fcoe port 2/1 role fcf-only`
- `no fcoe port 2/1`

**Release History**

Release 7.3.2; command introduced.
Related Commands

- **fcoe vlan**: Configures an FCoE VLAN.
- **show fcoe ports**: Displays the status and configuration of FCoE interfaces.

MIB Objects

- **alaFipsIntfTable**: Contains information about FCoE interfaces.
  - **alaFipsIntfIfIndex**: Interface index.
  - **alaFipsIntfOperStatus**: Operational status of the interface.
  - **alaFipsIntfPortRole**: Role of the port.
  - **alaFipsIntfRowStatus**: Status of the row.
**show fcoe**

Displays the global FCoE and FIP snooping status and configuration information for the switch.

```
show fcoe
```

---

**Syntax Definitions**
N/A

**Defaults**
N/A

**Platforms Supported**
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
N/A

**Examples**

```
-> show fcoe
```

FCoE Global Configurations:

```
FIP Snooping            : Disable,
Address-Mode            : FPMA,
Priority 1              : 3,
Priority 2              : -,
Priority Protection     : Enable,
Priority Protection Action: Drop,
Re-Mark Priority        : -,
Total Filter Resources  : 256,
Used Filter Resources   : 0,
Trap threshold (%)      : 80,
House Keeping Time Period : 300
```
**Output Definitions**

FIP Snooping - The administrative status of FIP snooping for the switch (Enable or Disable). Configured through the `fcoe fip-snooping` command.

Address-mode - Indicates whether a server-provided MAC address (SPMA) or a fabric-provided MAC address (FPMA) is assigned to virtual FCoE entities. Configured through the `fcoe address-mode` command.

Priority 1 - One of two global lossless priority values for FCoE traffic. Configured through `fcoe priority` command.

Priority 2 - Two of two global lossless priority values for FCoE traffic. Configured through `fcoe priority` command.

Priority Protection - The status of priority protection for the switch (Enable or Disable). Configured through the `fcoe priority-protection` command.

Priority Protection Action - The action applied to traffic that does not match the FCoE/FIP Ethertype and configured FCoE priority value (Drop or Remark). Configured through the `fcoe priority-protection action` command.

Re-mark Priority - The priority value to use for marking traffic that does not match the FCoE/FIP Ethertype and configured FCoE priority value. This value is only applied when the priority protection action is set to Remark. Configured through the `fcoe priority-protection action` command.

Total Filtering Resources - The number of ACL entries available for filtering of FCoE traffic.

Used Filtering Resources - The number of ACL entries currently in use for filtering FCoE traffic.

Trap threshold (%) - The percentage of filtering resources used for FIP. When this percentage is reached, a trap is sent indicating the available and maximum percentage of filtering resources. Configured through the `fcoe filtering-resource trap-threshold` command.

House Keeping Time Period - The amount of time the FCoE switch will wait to receive keep alive messages from the ENode and FCF. When this amount of time expires, information for the specific FCoE session is removed. Configured through the `fcoe house-keeping-time-period` command.

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- `show fcoe ports` - Displays the FCoE port configuration for the switch.
- `show fcoe sessions` - Displays the status and configuration of the FIP snooping sessions.

**MIB Objects**

- `alaFipsConfig`  
  - `alaFipsInfo`  
  - `alaFipsConfigFIPSAdmin`  
  - `alaFipsConfigAddressMode`  
  - `alaFipsConfigPriorityOne`  
  - `alaFipsConfigPriorityTwo`
alaFipsTotalNumFilterResource
alaFipsUsedNumFilterResource
alaFipsConfigHouseKeepingTimePeriod

NOTIFICATIONS (TRAPS)
alaFipsResourceThresholdReached
**show fcoe ports**

Displays the FCoE interface configuration for the switch.

```shell
-> show fcoe ports
```

<table>
<thead>
<tr>
<th>Ports</th>
<th>FCoE Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/3</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/4</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/5</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/6</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/7</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/11</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/13</td>
<td>Edge Port</td>
<td>ENABLED</td>
</tr>
<tr>
<td>1/14</td>
<td>Edge Port</td>
<td>ENABLED</td>
</tr>
<tr>
<td>1/15</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/19</td>
<td>FCF Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>2/1</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>2/8</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>0/1</td>
<td>Mixed Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>0/12</td>
<td>Mixed Port</td>
<td>ENABLED</td>
</tr>
<tr>
<td>0/40</td>
<td>Mixed Port</td>
<td>DISABLE</td>
</tr>
</tbody>
</table>

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command also shows the FCoE role assigned to the interface.

**Examples**

```shell
-> show fcoe ports
```

<table>
<thead>
<tr>
<th>Ports</th>
<th>FCoE Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/3</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/4</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/5</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/6</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/7</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/11</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/13</td>
<td>Edge Port</td>
<td>ENABLED</td>
</tr>
<tr>
<td>1/14</td>
<td>Edge Port</td>
<td>ENABLED</td>
</tr>
<tr>
<td>1/15</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>1/19</td>
<td>FCF Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>2/1</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>2/8</td>
<td>Edge Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>0/1</td>
<td>Mixed Port</td>
<td>DISABLE</td>
</tr>
<tr>
<td>0/12</td>
<td>Mixed Port</td>
<td>ENABLED</td>
</tr>
<tr>
<td>0/40</td>
<td>Mixed Port</td>
<td>DISABLE</td>
</tr>
</tbody>
</table>
FIP Snooping Commands

show fcoe ports

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Role</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/50</td>
<td>Mixed Port</td>
<td>ENABLED</td>
</tr>
</tbody>
</table>

**output definitions**

- **Ports**: The slot/port or link aggregate ID of the FCoE interface. A “0” slot number indicates that the FCoE interface is a link aggregate.
- **FCoE Role**: The designated role of the FCoE interface (Edge Port, ENode Port, FCF Port, Mixed Port, or Trusted Port).
- **Status**: The operational status of the FCoE interface (ENABLE or DISABLE).

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- **fcoe role**: Configures a port or link aggregate as an FCoE interface.
- **show fcoe**: Displays the FCoE and FIP status and configuration for the switch.

**MIB Objects**

AlaFipsIntfTable
- alaFipsIntfIfIndex
- alaFipsIntfOperStatus
- alaFipsIntfPortRole
- alaFipsIntfRowStatus
show fcoe sessions

Displays the FIP snooping session status and configuration for the switch.

```
show fcoe sessions [[fips | npiv-proxy | r-npiv] [port chassis/slot/port] | vlan vlan_id | linkagg agg_id] |
[e-tunnel [tunnel_id]]
```

Syntax Definitions

- **fips** Displays FIP snooping sessions on FCoE ports.
- **npiv-proxy** Displays N_Port proxy (NPIV) sessions between ENode and FC switch.
- **r-npiv** Displays F_Port proxy (R-NPIV) sessions between the HBA and the gateway switch.
- **chassis** The chassis identifier.
- **slot/port** The slot and port number (3/1).
- **vlan_id** An existing FCoE VLAN ID. The valid ID range is 2–4094.
- **agg_id** The link aggregate ID number.
- **tunnel_id** Displays E2E tunnel sessions between two E_Ports on different FC switches. Optionally enter a tunnel ID to display information for a specific tunnel.

Defaults

By default, all FCoE sessions are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `port` or `linkagg` parameter to display sessions for a specific FCoE port or link aggregate ID.
- Use the `vlan` parameter to display the sessions for a specific FCoE VLAN ID.
- The output displays for this command include FIP snooping, N_Port proxy (NPIV), F_Port proxy (reverse-NPIV), and E2E tunnel sessions. However, the N_Port proxy, F_Port proxy, and E2E tunnel sessions are only displayed on an OmniSwitch 6900 that is configured as an FCoE/FC gateway (see Chapter 44, “FCoE/FC Gateway Commands” for more information.
Examples

-> show fcoe sessions
Total FIP Snooping Sessions: 2
| PORT   | ENODE MAC       | VN_PORT MAC         | FCF MAC           | VLAN   | STATUS |
|--------+-----------------+-----------------+--------------------+----+---------|
| 1/1    | 00:00:00:11:22:33 0E:FC:00:00:00:05 00:AAB:B00:00:05 | 100 SUCCESS |
| 1/1    | 00:00:00:11:22:33 00:00:00:00:00:00 00:AAB:B00:00:05 | 100 PENDING |

Total NPIV Sessions: 1
| IN-PORT VLAN | ENODE_MAC       | VN_PORT_MAC         | FCF MAC       | STATUS | OUT-PORT |
|--------------+-----------------+-----------------+-----------------+-------+--------|
| 1/1          | 100 00:00:00:11:23:34 0E:FC:00:00:00:00 00:AAB:0103:01 | PENDING 2/1 |

Total R-NPIV Sessions: 2
| IN-PORT VLAN VSAN | FCID     | VN_PORT_MAC         | FCF MAC       | STATUS | OUT-PORT |
|------------------+---------+-----------------+-----------------+-------+--------|
| 2/2              | 400 01:02:02 | 0E:FC:00:01:02:02 00:AAB:0102:02 | SUCCESS 1/2 |
| 2/3              | - 01:03:01 | - | SUCCESS 2/1 |

Total E-TUNNEL sessions: 3
| TUNNEL-ID | PORT1 | PORT2 |_VLAN | PAIR MODE | FCF MAC | STATUS |
|-----------+-------+-------+-------+-----------+---------+---------|
| 1         | 2/12  | 2/12  | -     | TE to TE  | -       | SUCCESS |
| 10        | 2/3   | 1/4   | 10    | TE to VE  | 00:E0:B1:71:23:12 | SUCCESS |
| 20        | 2/4   | 1/5   | 300   | TE to VE  | 00:E0:B1:71:23:10 | SUCCESS |

-> show fcoe sessions fips
Total FIP Snooping Sessions: 2
| PORT   | ENODE MAC       | VN_PORT MAC         | FCF MAC           | VLAN   | STATUS |
|--------+-----------------+-----------------+--------------------+----+---------|
| 1/1    | 00:00:00:11:22:33 0E:FC:00:00:00:05 00:AAB:B00:00:05 | 100 SUCCESS |
| 1/1    | 00:00:00:11:22:33 00:00:00:00:00:00 00:AAB:B00:00:05 | 100 PENDING |

-> show fcoe sessions npiv-proxy
Total NPIV Sessions: 1
| IN-PORT VLAN | ENODE_MAC       | VN_PORT_MAC         | FCF MAC       | STATUS | OUT-PORT |
|--------------+-----------------+-----------------+-----------------+-------+--------|
| 1/1          | 100 00:00:00:11:23:34 0E:FC:00:00:00:00 00:AAB:00:01:03:01 | PENDING 2/1 |

-> show fcoe sessions r-npiv
Total R-NPIV Sessions: 2
| IN-PORT VLAN VSAN | FCID     | VN_PORT_MAC         | FCF MAC       | STATUS | OUT-PORT |
|------------------+---------+-----------------+-----------------+-------+--------|
| 2/2              | 400 01:02:02 | 0E:FC:00:01:02:02 00:AAB:0102:02 | SUCCESS 1/2 |
| 2/3              | - 01:03:01 | - | SUCCESS 2/1 |

-> show fcoe sessions e-tunnel
Total E-TUNNEL sessions: 3
| TUNNEL-ID | PORT1 | PORT2 | VLAN | PAIR MODE | FCF MAC | STATUS |
|-----------+-------+-------+-------+-----------+---------+---------|
| 1         | 2/12  | 2/12  | -     | TE to TE  | -       | SUCCESS |
| 10        | 2/3   | 1/4   | 10    | TE to VE  | 00:E0:B1:71:23:12 | SUCCESS |
| 20        | 2/4   | 1/5   | 300   | TE to VE  | 00:E0:B1:71:23:10 | SUCCESS |
-> show fcoe sessions e-tunnel 10
Total E-TUNNEL sessions: 3
TUNNEL-ID PORT1 PORT2 VLAN PAIR MODE FCF MAC STATUS
-------------------+--------+--------+-------+-----------+-----------------+---------
 10            2/3     1/4    10      TE to VE   00:E0:B1:71:23:12  SUCCESS

-> show fcoe sessions vlan 10
Total FIP Snooping Sessions : 2
Total FIP Snooping Sessions on VLAN 10 : 1
PORT ENODE MAC VN_PORT MAC FCF MAC VLAN STATUS
-------+-----------------+-----------------+-----------------+----+---------
 1/1   00:00:00:11:22:33 0E:FC:00:00:00:05 00:AA:BB:00:00:05    10  SUCCESS

Total NPIV Sessions : 3
Total NPIV Sessions on VLAN 10 : 1
IN-PORT VLAN ENODE_MAC VN_PORT_MAC FCF MAC STATUS OUT-PORT
-------+----+-----------------+-----------------+-----------------+-------+--------
 1/1    10 00:00:00:11:23:34 0E:FC:00:00:00:00 00:AA:00:01:03:01 PENDING 2/1

Total R-NPIV Sessions : 3
Total R-NPIV Sessions on VLAN 10 : 1
IN-PORT VLAN VSAN FCID VN_PORT_MAC FCF MAC STATUS OUT-PORT
-------+----+----+--------+-----------------+-----------------+---------+--------
 2/2   10 400 01:02:02 0E:FC:00:01:02:02 00:AA:00:01:02:02 SUCCESS 1/2

Total E-TUNNEL Sessions : 3
Total E-TUNNEL Sessions on VLAN 10 : 1
TUNNEL-ID PORT1 PORT2 VLAN PAIR MODE FCF MAC STATUS
-------------------+--------+--------+-------+-----------+-----------------+---------
 10            2/3     1/4    10      TE to VE   00:E0:B1:71:23:12  SUCCESS

-> show fcoe sessions fips port 1/1
Total FIP Snooping Sessions : 4
Total FIP Snooping Sessions on Port 1/1 : 2
PORT ENODE MAC VN_PORT MAC FCF MAC VLAN STATUS
-------+-----------------+-----------------+-----------------+----+---------
 1/1   00:00:00:11:22:33 0E:FC:00:00:00:05 00:AA:BB:00:00:05    100 SUCCESS
 1/1   00:00:00:11:22:33 00:00:00:00:00:00 00:AA:BB:00:00:05    100 PENDING

-> show fcoe sessions npiv linkagg 1
Total NPIV Sessions : 3
Total NPIV Sessions on Linkagg 1 : 1
IN-PORT VLAN ENODE_MAC VN_PORT_MAC FCF MAC STATUS OUT-PORT
-------+----+-----------------+-----------------+-----------------+-------+--------
 0/10 100 00:00:00:11:23:34 0E:FC:00:00:00:00 00:AA:00:01:03:01 PENDING 2/1

output definitions

**PORT**
The FCoE port or link aggregate ID for a FIP snooping session. A “0” slot number indicates that the FCoE interface is a link aggregate.
Configured through the `fcoe role` command.

**ENODE MAC**
The MAC address of the ENode for this session.

**VN_PORT MAC**
The MAC address of the virtual node (VN) port for this session.

**FCF MAC**
The MAC address of the FCoE Forwarder (FCF) for this session.
### Output Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>The FCoE VLAN used for this session. Configured through the <code>fcoe vlan</code> command.</td>
</tr>
<tr>
<td>STATUS</td>
<td>The operational status of this session.</td>
</tr>
<tr>
<td>IN-PORT</td>
<td>The FCoE port or link aggregate ID for an N_Port proxy (NPIV) or F_Port proxy (R-NPIV) session. Configured through the <code>fcoe role</code> command.</td>
</tr>
<tr>
<td>OUT-PORT</td>
<td>The FC port for an N_Port proxy (NPIV) or F_Port proxy (R-NPIV) session. Configured through the <code>fibre-channel port mode</code> command.</td>
</tr>
<tr>
<td>VSAN</td>
<td>The VSAN ID mapped to the FCoE VLAN ID for an F_Port proxy (R-NPIV) session. Configured through the <code>fibre-channel vsan</code> command.</td>
</tr>
<tr>
<td>FCID</td>
<td>The FC port ID (also referred to as N_Port ID) received after successful login for an F_Port proxy (R-NPIV) session.</td>
</tr>
<tr>
<td>TUNNEL-ID</td>
<td>The E2E tunnel ID associated with the session. Configured through the <code>fcoe e-tunnel</code> command.</td>
</tr>
<tr>
<td>PORT1, PORT2</td>
<td>The FCoE port (in VE_Port role) and/or FC port (in TE_Port mode) for this session. The FCoE port rule is configured through the <code>fcoe role</code> command. The FC port mode is configured through the <code>fibre-channel port mode</code> command.</td>
</tr>
<tr>
<td>PAIR MODE</td>
<td>The type of E2E tunnel (TE to VE or TE to TE).</td>
</tr>
</tbody>
</table>

### Release History

Release 7.3.2; command introduced.
Release 7.3.3; fields added to display NPIV, reverse-NPIV, and E2E tunnel sessions.

### Related Commands

- `show fcoe`: Displays the global FCoE and FIP snooping configuration for the switch.
- `show fcoe ports`: Displays the FCoE port configuration for the switch.
- `show fibre-channel port`: Displays the FC port configuration for the switch.
**MIB Objects**

AlaFipsSessionTable
   alaFipsSessionEnodeMAC
   alaFipsSessionVNNMAC
   alaFipsSessionVlanId
   alaFipsSessionIfIndex
   alaFipsSessionFCFMAC

AlaFipsNpivSessionTable
   alaFipsNpivSessionEnodeMAC
   alaFipsNpivSessionVNNMAC
   alaFipsNpivSessionVlanId
   alaFipsNpivSessionInIfIndex
   alaFipsNpivSessionOutIfIndex
   alaFipsNpivSessionFCFMAC

AlaFipsRnpivSessionTable
   alaFipsRnpivSessionVNNMAC
   alaFipsRnpivSessionVlanId
   alaFipsRnpivSessionInIfIndex
   alaFipsRnpivSessionOutIfIndex
   alaFipsRnpivSessionFCFMAC
   alaFipsRnpivSessionStatus
   alaFipsRnpivSessionVsanId
   alaFipsRnpivSessionFcId

AlaFipsEtunnelSessionTable
   alaFipsEtunnelSessionTunnelId
   alaFipsEtunnelSessionVlanId
   alaFipsEtunnelSessionInIfIndex
   alaFipsEtunnelSessionOutIfIndex
   alaFipsEtunnelSessionFCFMAC
   alaFipsEtunnelSessionStatus
   alaFipsEtunnelSessionPairMode
show fcoe enode

Displays FCoE Node (ENode) information for FIP Snooping sessions associated with the switch.

show fcoe enode [mac_address]

Syntax Definitions

mac_address Enter an ENode MAC Address (for example, 00:00:39:59:f1:0c).

Defaults

By default, information is displayed for all ENodes associated with the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Specify an ENode MAC address to display more detailed information about a specific ENode.

Examples

-> show fcoe enode
Port   Enode MAC         VLAN       Sessions
----+-------------------+-----+-------------
1/1  00:10:00:00:00:02    100             2
2/1  00:00:a0:bb:00:01    200             1

-> show fcoe enode 00:10:00:00:00:02
Enode MAC: 00:10:00:00:00:02 Port : 1/1

VN-Port-MAC          FCF-MAC       Vlan     Login time
-------------------+------------------+----+--------------------------
0E:FC:00:00:00:15   00:AE:00:00:00:01  100  Thu Feb 14 07:22:54 2013
0E:FC:00:00:00:09   0E:AE:00:00:00:01  200  Thu Feb 14 07:12:22 2013

output definitions

Port The slot/port or link aggregate ID of the FCoE interface that is connected to the FCoE Node (ENode). A “0” slot number indicates that the FCoE interface is a link aggregate.

Enode MAC The MAC address of the ENode connected to the FCoE interface.

VLAN The FCoE VLAN ID.
output definitions

<table>
<thead>
<tr>
<th>Sessions</th>
<th>The number of sessions associated with the ENode MAC.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VN-Port-MAC</td>
<td>The MAC address of the virtual node port (VN_port) for this session.</td>
</tr>
<tr>
<td>FCF-MAC</td>
<td>The MAC address of the FCoE Forwarder (FCF).</td>
</tr>
<tr>
<td>Login time</td>
<td>The date and time the ENode logged into the FCoE fabric.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command introduced.

Related Commands

- **show fcoe sessions**: Displays FCoE FIP snooping session status and configuration for the switch.
- **show fcoe fcf**: Displays FCoE Forwarder (FCF) information for the switch.

MIB Objects

- **alaFipsSessionTable**
  - **alaFipsSessionEnodeMAC**
  - **alaFipsSessionVNMAC**
  - **alaFipsSessionVlanId**
  - **alaFipsSessionIfIndex**
  - **alaFipsSessionFCFMAC**
  - **alaFipsSessionLoginTime**
**show fcoe fcf**

Displays FCoE Forwarder (FCF) information for FIP Snooping sessions associated with the switch.

```
show fcoe fcf [mac_address]
```

### Syntax Definitions

- **mac_address**
  
Enter an FCF Address (for example, 00:00:39:59:f1:0c).

### Defaults

By default, information is displayed for all FCFs associated with the switch.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

Specify an FCF MAC address with this command to display more detailed information for a specific FCF.

### Examples

```
-> show fcoe fcf

<table>
<thead>
<tr>
<th>FCF-MAC</th>
<th>VLAN</th>
<th>Config</th>
<th>Sessions</th>
<th>A-bit</th>
<th>MaxFrmVer</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>E8:E7:32:3F:FD:F0</td>
<td>46</td>
<td>Npiv</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>E8:E7:32:63:8B:B0</td>
<td>56</td>
<td>Dynamic</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>128</td>
</tr>
<tr>
<td>E8:E7:32:94:68:17</td>
<td>4000</td>
<td>Dynamic</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>128</td>
</tr>
<tr>
<td>E8:E7:32:94:68:E8</td>
<td>3000</td>
<td>Static</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>E8:E7:32:94:68:EE</td>
<td>4000</td>
<td>Static</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

-> show fcoe fcf E8:E7:32:3F:FD:F0

FCF : E8:E7:32:3F:FD:F0

<table>
<thead>
<tr>
<th>VLAN</th>
<th>VN-Port-MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>0E:FC:00:01:00:03</td>
</tr>
<tr>
<td>46</td>
<td>0E:FC:00:01:00:80</td>
</tr>
<tr>
<td>46</td>
<td>0E:FC:00:01:00:82</td>
</tr>
<tr>
<td>46</td>
<td>0E:FC:00:01:00:81</td>
</tr>
</tbody>
</table>
```

**output definitions**

- **FCF-MAC**
  
The MAC address of the FCoE Forwarder (FCF).

- **VLAN**
  
The FCoE VLAN ID.
**output definitions**

<table>
<thead>
<tr>
<th>Config</th>
<th>Whether the FCF MAC address was user-configured or learned through the FIP Snooping session for the given FCoE VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sessions</td>
<td>The number of sessions associated with the FCF MAC for the given FCoE VLAN.</td>
</tr>
<tr>
<td>A-bit</td>
<td>Whether or not the available-for-login bit is set for this FCF.</td>
</tr>
<tr>
<td>MaxFrmVer</td>
<td>Whether or not the maximum frame size was verified for this FCF.</td>
</tr>
<tr>
<td>VN-Port-MAC</td>
<td>The MAC address of the virtual node port (VN_Por) for this session. This address is comprised of the FCID that the FCF assigned to the port combined with the FC-MAP.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.2; command introduced.
Release 7.3.3; **A-bit** and **MaxFrmVer** fields added.

**Related Commands**

- **show fcoe sessions**  
  Displays FCoE FIP snooping session status and configuration for the switch.

- **show fcoe enode**  
  Displays FCoE Node (ENode) information for the switch.

**MIB Objects**

- alaFipsFcfTable
  - alaFipsFcfSessions
  - alaFipsSessionFCFMAC
  - alaFipsSessionVlanId
  - alaFipsFcfConfigType
  - alaFipsFcfAvailForLogin
  - alaFipsFcfMaxFcoeFrmSizeVerified
show fcoe fc-map

Displays the Fibre Channel Mapped Address Prefix (FC-MAP) for each FCoE VLAN.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the FCoE address mode is set to Fabric-Provided MAC Address (FPMA), the FC-MAP value is the required upper 24 bits of a MAC address that is assigned to a Virtual N_Port (VN_Port).

**Examples**

```
-> show fcoe fc-map
    VLAN   FC-MAP
    --------+--------
        10   0E:FC:00
        100  0E:FC:22
        200  0E:FC:23
        300  0E:FC:23
```

**Release History**

Release 7.3.2; command introduced.
Related Commands

- **fcoe vlan**: Configures an FCoE VLAN for the switch.
- **fcoe fc-map**: Configures the FC-MAP for an FCoE VLAN.
- **show vlan**: Displays the VLAN configuration for the switch.

MIB Objects

- **alaFipsVlanTable**
  - **alaFipsVlanId**
  - **alaFipsVlanFCMap**
**show fcoe discovery-advertisement**

Displays the FIP discovery advertisement message parameter values for the specified FCoE VLAN.

```
show fcoe discovery-advertisement [vlan vlan_id[-vlan_id2]]
```

**Syntax Definitions**

```
vlan_id[-vlan_id2] An existing FCoE VLAN ID. Use a hyphen to specify a range of FCoE VLAN IDs (10-25).
```

**Defaults**

By default, the discovery advertisement parameters are displayed for all FCoE VLANs.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `vlan_id[-vlan_id2]` parameter to display information for a specific FCoE VLAN or for a range of FCoE VLANs.

**Examples**

```
-> show fcoe discovery-advertisement
VLAN A-Bit FKA Pd Priority UDS-Retries
----------+--------+----------+--------+--------------
 46 ENABLE 8  128      3
 56 ENABLE 8  128      3
 76 ENABLE 8  128      3
3000 ENABLE 8  128      3
4000 ENABLE 8  128      3

-> show fcoe discovery-advertisement vlan 3000
VLAN A-Bit FKA Period Priority UDS-Retries
----------+--------+----------+--------+--------------
 3000 ENABLE 8  128      3
```

**output definitions**

- **VLAN**: The FCoE VLAN ID. Configured through the `fcoe vlan` command.
- **A-Bit**: The status of the available-for-login bit (Enabled or Disabled). When enabled, indicates the switch can accept fabric logins from ENodes.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FKA-PD</td>
<td>The discovery advertisement transmission interval, in seconds.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority value assigned to the switch (0 = highest priority, 255 = lowest priority).</td>
</tr>
<tr>
<td>UDS-Retries</td>
<td>The number of times a unicast discovery solicitation is transmitted after a port on which an FCF MAC was learned goes down.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command introduced.

**Related Commands**

`fcoe discovery-advertisement` Configures FIP discovery advertisement parameter values.

**MIB Objects**

alaFipsDiscAdvtTable
- alaFipsDiscAdvtVlanId
- alaFipsDiscAdvtAbit,
- alaFipsDiscAdvtFkaAdvPeriod,
- alaFipsDiscAdvtPriority,
- alaFipsDiscAdvtUdsRetries,
- alaFipsDiscAdvtRowStatus
**show fcoe statistics**

Displays both ENode and FCF generated statistics for FCoE interfaces or specific VLANs.

```
```

**Syntax Definitions**

- **enode**: Display statistics only for ENode traffic.
- **fcf**: Display statistics only for FCF traffic.
- **interface**: Display statistics for all FCoE interfaces (ports and link aggregates).
- **vlan_id|vlan_id2**: An existing FCoE VLAN ID. Use a hyphen to specify a range of FCoE VLAN IDs (10-25).
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

By default, FCF and ENode statistics are displayed for all FCoE interfaces and VLANs.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **vlan** parameter to display statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to display statistics for a specific FCoE port or link aggregate ID.
- The output displays for this command include FIP snooping, N_Port proxy (NPIV), and F_Port proxy (reverse-NPIV) statistics. However, the N_Port proxy and F_Port proxy statistics are only displayed on an OmniSwitch 6900 that is configured as an FCoE/FC gateway (see Chapter 44, “FCoE/FC Gateway Commands” for more information.)
## Examples

-> show fcoe statistics interface

### Enode Statistics

<table>
<thead>
<tr>
<th>Port</th>
<th>Sess</th>
<th>VL REQ</th>
<th>MDS</th>
<th>UDS</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>LOGO</th>
<th>E KA</th>
<th>VN KA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### FCF Statistics

<table>
<thead>
<tr>
<th>Port</th>
<th>Sess</th>
<th>VL RESP</th>
<th>MDA</th>
<th>UDA</th>
<th>FLOGI_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_ACC</th>
<th>FDISC_RJT</th>
<th>LOGO_ACC</th>
<th>LOGO_RJT</th>
<th>CVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td>0</td>
<td>0</td>
<td>32997</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### NPIV Enode-Discovery Statistics

**Packets Received:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan Req</th>
<th>MDS</th>
<th>UDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan Res</th>
<th>MDA</th>
<th>UDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### NPIV Enode-Login Statistics

**Packets Received:**

<table>
<thead>
<tr>
<th>Port</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>LOGO</th>
<th>E_KA</th>
<th>VN_KA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>Port</th>
<th>FLOGI_ACC</th>
<th>FDISC_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_RJT</th>
<th>LOGO_RJT</th>
<th>CVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

### R-NPIV FCF-Discovery Statistics

**Packets Received:**

<table>
<thead>
<tr>
<th>Port</th>
<th>MDA</th>
<th>UDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td>32991</td>
<td>1</td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>Port</th>
<th>MDS</th>
<th>UDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

### R-NPIV Node-Login Statistics

**Packets Received:**

<table>
<thead>
<tr>
<th>Port</th>
<th>FLOGI_ACC</th>
<th>FDISC_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_RJT</th>
<th>CVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>Port</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>LOGO</th>
<th>VN-KA</th>
<th>E-KA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/17</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2952</td>
<td>33191</td>
</tr>
</tbody>
</table>

-> show fcoe statistics enode interface

### Enode Statistics

<table>
<thead>
<tr>
<th>Port</th>
<th>Sess</th>
<th>MDS</th>
<th>UDS</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>LOGO</th>
<th>E KA</th>
<th>VN KA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
-> show fcoe statistics vlan

Enode Statistics

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Sess</th>
<th>MDS</th>
<th>UDS</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>LOGO</th>
<th>E KA</th>
<th>VN KA</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0</td>
<td>0</td>
<td>3314</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

FCF Statistics

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Sess</th>
<th>MDA</th>
<th>UDA</th>
<th>FLOGI_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_ACC</th>
<th>FDISC_RJT</th>
<th>LOGO_ACC</th>
<th>LOGO_RJT</th>
<th>CVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

NPV Enode-Discovery Statistics

Packets Received:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Vlan Req</th>
<th>MDS</th>
<th>UDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Packets Sent:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Vlan Res</th>
<th>MDA</th>
<th>UDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

NPV Enode-Login Statistics

Packets Received:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>LOGO</th>
<th>E_KA</th>
<th>VN_KA</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Packets Sent:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>FLOGI_ACC</th>
<th>FDISC_ACC</th>
<th>FLOGO_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_RJT</th>
<th>FLOGO_RJT</th>
<th>CVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>118</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

R-NPV FCF-Discovery Statistics

Packets Received:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MDA</th>
<th>UDA</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>33409</td>
<td>1</td>
</tr>
</tbody>
</table>

Packets Sent:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>MDS</th>
<th>UDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

R-NPV Node-Login Statistics

Packets Received:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>FLOGI_ACC</th>
<th>FDISC_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_RJT</th>
<th>CVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Packets Sent:

<table>
<thead>
<tr>
<th>Vlan</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>LOGO</th>
<th>VN-KA</th>
<th>E-KA</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2990</td>
<td>33611</td>
</tr>
</tbody>
</table>

-> show fcoe statistics fcf vlan

FCF Statistics

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Sess</th>
<th>MDA</th>
<th>UDA</th>
<th>FLOGI_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_ACC</th>
<th>FDISC_RJT</th>
<th>LOGO_ACC</th>
<th>LOGO_RJT</th>
<th>CVL</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The slot/port or link aggregate ID of the FCoE interface. A &quot;0&quot; slot number indicates that the FCoE interface is a link aggregate.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sess</td>
<td>The number of FIP Snooping sessions.</td>
</tr>
<tr>
<td>MDS</td>
<td>The number of Multicast Discovery Solicitation packets.</td>
</tr>
<tr>
<td>UDS</td>
<td>The number of Unicast Discovery Solicitation packets.</td>
</tr>
<tr>
<td>FLOGI</td>
<td>The number of Fabric Login packets.</td>
</tr>
<tr>
<td>FDISC</td>
<td>The number of Fabric Discovery packets.</td>
</tr>
<tr>
<td>LOGO</td>
<td>The number of Fabric Logout packets.</td>
</tr>
<tr>
<td>E KA</td>
<td>The number of ENode keep-alive packets.</td>
</tr>
<tr>
<td>VN KA</td>
<td>The number of VN_Port keep-alive packets.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The FCoE VLAN ID.</td>
</tr>
<tr>
<td>MDA</td>
<td>The number of Multicast Discovery Advertisement packets.</td>
</tr>
<tr>
<td>UDA</td>
<td>The number of Unicast Discovery Advertisement packets.</td>
</tr>
<tr>
<td>FLOGI_ACC</td>
<td>The number of Fabric Login Accept packets.</td>
</tr>
<tr>
<td>FLOGI_RJT</td>
<td>The number of Fabric Login Reject packets.</td>
</tr>
<tr>
<td>FDISC_ACC</td>
<td>The number of Fabric Discovery Accept packets.</td>
</tr>
<tr>
<td>FDISC_RJT</td>
<td>The number of Fabric Discover Reject packets.</td>
</tr>
<tr>
<td>LOGO_ACC</td>
<td>The number of Fabric Logout Accept packets.</td>
</tr>
<tr>
<td>LOGO_RJT</td>
<td>The number of Fabric Logout Reject packets.</td>
</tr>
<tr>
<td>CVL</td>
<td>The number of Clear Virtual Link packets.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command introduced.  
Release 7.3.3; N_Port proxy and F_Port proxy statistics displayed only on an OmniSwitch 6900.

Related Commands

clear fcoe statistics  
Clears ENode and FCF statistics.

MIB Objects

alaFipsIntfEnodeStatsTable  
alaFipsIntfFcfStatsTable  
alaFipsVlanEnodeStatsTable  
alaFipsVlanFcfStatsTable
clear fcoe statistics

Clears ENode and FCF generated statistics on FCoE interfaces or specific VLANs.

clear fcoe statistics [enode | fcf] [interface | vlan [vlan_id[|vlan_id2]] | port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]

Syntax Definitions

enode
  Clears statistics only for ENode traffic.
fcf
  Clears statistics only for FCF traffic.
interface
  Clears statistics on all FCoE interfaces (ports and link aggregates).
vlans vlan_id[|vlan_id2]
  An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a
  hyphen to specify a range of VLAN IDs (100-150).
chassis
  The chassis identifier.
slot/port[-port2]
  The slot and port number (3/1). Use a hyphen to specify a range of ports
  (3/1-8).
linkagg agg_id[-agg_id2]
  The link aggregate ID number. Use a hyphen to specify a range of IDs
  (10-20).

Defaults

By default, statistics are cleared for all FCoE interfaces and VLANs.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the port or linkagg parameters to clear the statistics for a specific FCoE port or link aggregate ID.
- Use the vlan parameter to clear the statistics for a specific FCoE VLAN ID.

Examples

- clear fcoe statistics
- clear fcoe statistics interface
- clear fcoe statistics vlan
- clear fcoe statistics vlan 2
- clear fcoe statistics vlan 2-3
- clear fcoe statistics port 1/2
-> clear fcoe statistics port 1/2-3
-> clear fcoe statistics port 1/1/2
-> clear fcoe statistics linkagg 2
-> clear fcoe statistics linkagg 2-6
-> clear fcoe statistics enode interface
-> clear fcoe statistics enode vlan
-> clear fcoe statistics enode vlan 2
-> clear fcoe statistics enode vlan 2-3

-> clear fcoe statistics enode port 1/2
-> clear fcoe statistics enode port 1/2-3
-> clear fcoe statistics enode port 1/1/2
-> clear fcoe statistics enode port 1/1/2-3

-> clear fcoe statistics enode linkagg 2
-> clear fcoe statistics enode linkagg 2-6

-> clear fcoe statistics fcf interface
-> clear fcoe statistics fcf vlan
-> clear fcoe statistics fcf vlan 2
-> clear fcoe statistics fcf vlan 2-3

-> clear fcoe statistics fcf port 1/2
-> clear fcoe statistics fcf port 1/2-3
-> clear fcoe statistics fcf port 1/1/2
-> clear fcoe statistics fcf port 1/1/2-3

-> clear fcoe statistics fcf linkagg 2
-> clear fcoe statistics fcf linkagg 2-6

**Release History**

Release 7.3.2; command introduced.

**Related Commands**

*show fcoe statistics* Displays ENode and FCF statistics for FCoE interfaces and VLANs.

**MIB Objects**

alaFipsConfig
  alaFipsConfigStatsClear
alaFipsIntfTable
  alaFipsIntfStatsClear
alaFipsVlanTable
  alaFipsVlanStatsClear
The OmniSwitch implementation of FCoE/FC gateway functionality allows the switch to transparently connect FCoE and FC nodes with an FC SAN across an FCoE (lossless Ethernet) network. To provide this type of connectivity, an OmniSwitch FCoE/FC gateway supports the following three modes of operation that are used to converge FC over Ethernet and FC-to-FC over Ethernet:

- **N_Port Proxy mode**—allows ENodes in an FCoE network and FC switches in an FC SAN to communicate with each other. To an ENode the OmniSwitch gateway emulates an FCoE forwarder; to an FC switch the OmniSwitch gateway emulates an N_Port ID Virtualization (NPIV) host.

- **F_Port Proxy mode**—allows FC nodes to connect with FC switches and FCFs across an FCoE network. The OmniSwitch gateway forwards login requests from an FC node (N_Port on a server or storage with an HBA) across Ethernet via an FCoE VLAN to an NPIV node or FCF. This mode is sometimes referred to as reverse-NPIV proxy (R-NPIV).

- **E_Port Proxy mode**—allows FC switches to set up inter-switch link trunking between FC fabrics over an FCoE network. The OmniSwitch gateway provides an E_Port to E_Port (E2E) tunneling function that emulates a point-to-point FC link between E_Ports on native FC switches.

The OmniSwitch FCoE/FC gateway sits at the entry point of an FC fabric, which is required to handle the login process for ENodes and FC nodes accessing the fabric through the gateway switch.

OmniSwitch FCoE/FC gateway operations are not automatically activated for the switch; there is no single command to enable or disable gateway functionality. Instead, the configuration of the following software components enables one or more of the supported gateway operations:

- **FIP snooping**—FCoE/FC gateway functionality requires an active FIP snooping configuration. FIP Snooping ensures the security of an FCoE network.

- **Virtual Storage Area Network (VSAN)**—an FC port is assigned to a VSAN to create an NP_Port or F_Port connection to an FC switch or node in that VSAN. Not required for E2E Tunnel configuration.

- **VSAN-to-FCoE VLAN mapping**—identifies the FCoE/FC gateway fabric for the ENode or FC node login process via the FCoE VLAN. Not required for E_Port proxy (E2E Tunnel) configuration.

- **FC port mode**—the operational mode of the FC port determines the type of gateway functionality provided on that port. There are three modes supported: N_Port proxy, F_Port proxy, and E_Port proxy.

- **FCoE port role**—an FCoE port serves as an E2E tunnel endpoint in an FCoE network only when the port is configured as a virtual E_Port (VE_Port). The role of other FCoE ports is configured based on the FIP snooping configuration for the gateway switch.

This chapter and the Chapter 43, “FIP Snooping Commands,” describe the command line interface (CLI) commands used to configure these components.
MIB information for the FCoE/FC gateway commands is as follows:

Filename: ALCATEL-IND1-FIPS-MIB.mib
Module: alcatelIND1FipsMIB

The acronyms used in this chapter are defined here:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNA</td>
<td>Converged Network Adapter</td>
</tr>
<tr>
<td>CVL</td>
<td>Clear Virtual Link</td>
</tr>
<tr>
<td>E2E</td>
<td>E_Port-to-E_Port Tunnel</td>
</tr>
<tr>
<td>ELP</td>
<td>Exchange Link Parameters</td>
</tr>
<tr>
<td>ENode</td>
<td>FCoE Node</td>
</tr>
<tr>
<td>E_Port</td>
<td>Expansion Port</td>
</tr>
<tr>
<td>F_Port</td>
<td>Fabric Port</td>
</tr>
<tr>
<td>FC</td>
<td>Fibre Channel</td>
</tr>
<tr>
<td>FCF</td>
<td>FCoE Forwarder</td>
</tr>
<tr>
<td>FDISC</td>
<td>Fabric Discovery</td>
</tr>
<tr>
<td>FCID</td>
<td>Fabric Port ID (same as N_Port ID)</td>
</tr>
<tr>
<td>FCoE</td>
<td>Fibre Channel over Ethernet</td>
</tr>
<tr>
<td>FIP</td>
<td>FCoE Initialization Protocol</td>
</tr>
<tr>
<td>FLOGI</td>
<td>Fabric Login</td>
</tr>
<tr>
<td>FLOGO</td>
<td>Fabric Logout</td>
</tr>
<tr>
<td>HBA</td>
<td>Host Bus Adapter</td>
</tr>
<tr>
<td>ISL</td>
<td>Inter-switch Link</td>
</tr>
<tr>
<td>NPIV</td>
<td>N_Port ID Virtualization</td>
</tr>
<tr>
<td>N_Port</td>
<td>Node Port</td>
</tr>
<tr>
<td>NP_Port</td>
<td>Proxy Node Port</td>
</tr>
<tr>
<td>TE_Port</td>
<td>Tunnel Expansion Port</td>
</tr>
<tr>
<td>VE_Port</td>
<td>Virtual E_Port</td>
</tr>
<tr>
<td>VF_Port</td>
<td>Virtual F_Port</td>
</tr>
<tr>
<td>VN_Port</td>
<td>Virtual N_Port</td>
</tr>
<tr>
<td>VSAN</td>
<td>Virtual Storage Area Network</td>
</tr>
<tr>
<td>WWNN</td>
<td>World Wide Node Name</td>
</tr>
<tr>
<td>WWPN</td>
<td>World Wide Port Name</td>
</tr>
</tbody>
</table>
The FCoE/FC gateway commands are listed here:

<table>
<thead>
<tr>
<th>Configuration commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>fibre-channel vsan</td>
</tr>
<tr>
<td>fibre-channel port mode</td>
</tr>
<tr>
<td>fibre-channel vsan members</td>
</tr>
<tr>
<td>fcoe vsan-map</td>
</tr>
<tr>
<td>fibre-channel npiv-proxy load-balance</td>
</tr>
<tr>
<td>fibre-channel npiv-proxy load-balance static</td>
</tr>
<tr>
<td>fcoe e-tunnel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Show commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>show fibre-channel vsan</td>
</tr>
<tr>
<td>show fibre-channel vsan members</td>
</tr>
<tr>
<td>show fibre-channel port</td>
</tr>
<tr>
<td>show fcoe vsan-map</td>
</tr>
<tr>
<td>show fibre-channel sessions</td>
</tr>
<tr>
<td>show fibre-channel node</td>
</tr>
<tr>
<td>show fcoe e-tunnel</td>
</tr>
<tr>
<td>show fibre-channel</td>
</tr>
<tr>
<td>show fibre-channel npiv-proxy load-balance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Statistics commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>show fibre-channel statistics</td>
</tr>
<tr>
<td>show fcoe statistics npiv-proxy</td>
</tr>
<tr>
<td>show fcoe statistics r-npiv</td>
</tr>
<tr>
<td>show fcoe statistics e-tunnel</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clear commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear fibre-channel statistics</td>
</tr>
<tr>
<td>clear fibre-channel sessions</td>
</tr>
<tr>
<td>clear fcoe statistics npiv</td>
</tr>
<tr>
<td>clear fcoe statistics r-npiv</td>
</tr>
<tr>
<td>clear fcoe statistics e-tunnel</td>
</tr>
<tr>
<td>clear fcoe sessions</td>
</tr>
</tbody>
</table>
fibre-channel vsan

Configures an OmniSwitch VSAN with the specified VSAN ID and an optional description. This type of VSAN is used to segment OmniSwitch Fibre Channel ports into a virtual FCoE/FC gateway fabric.

**Note.** The VSAN created with this command only applies to the local switch configuration. There is no correlation between an OmniSwitch VSAN and a VSAN created within a native FC SAN.

```
fibre-channel vsan {vsan_id[-vsan_id2]} [admin-state {enable | disable}] [name description]
```

```
no fibre-channel vsan {vsan_id[-vsan_id2]}
```

### Syntax Definitions

- **vsan_id[-vsan_id2]**: A numeric value that will uniquely identify the VSAN. Use a hyphen to specify a range of VSAN IDs (for example, 100-105). The valid range is 2–4094).
- **enable**: Enable the VSAN administrative status.
- **disable**: Disable the VSAN administrative status.
- **description**: An alphanumeric string. Optional name description for the VSAN ID.

### Defaults

By default, VSAN 1 is created on the switch and all unassigned FC ports are assigned to VSAN 1.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>name</td>
<td>description</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete a VSAN from the configuration.
- When a VSAN is administratively disabled, all sessions established over that VSAN are cleared and the switch stops sending periodic FIP multicast discovery advertisement messages for the corresponding FCoE VLAN.
- The description can be any alphanumeric string. Enclose the description in double quotes if it contains more than one word with space in between.
Only FC switch ports can be assigned to a VSAN.

Assigning multiple FC ports to the same VSAN is allowed, but an FC port can only belong to one VSAN.

Configuring N_Port and F_Port proxy functionality requires mapping a VSAN to an FCoE VLAN. Note that only one VSAN is mapped to one FCoE VLAN (one-to-one) at any given time. This mapping defines a single traffic path through the gateway switch.

If an FCoE VLAN is not mapped to a VSAN, then the FCoE VLAN participates only in the FIP snooping process.

Examples

-> fibre-channel vsan 200 name “Fabric A”
-> fibre-channel vsan 100-105 admin-state disable
-> no fibre-channel vsan 200

Release History

Release 7.3.3; command introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fibre-channel vsan members</td>
<td>Assigns FC switch ports to a VSAN.</td>
</tr>
<tr>
<td>fcoe vsan-map</td>
<td>Maps a VSAN to an FCoE VLAN.</td>
</tr>
<tr>
<td>show fibre-channel vsan</td>
<td>Displays the VSAN configuration for the switch.</td>
</tr>
<tr>
<td>show fcoe vsan-map</td>
<td>Displays the VSAN-VLAN mapping configuration for the switch.</td>
</tr>
<tr>
<td>show fibre-channel vsan members</td>
<td>Displays FC port assignments for each VSAN.</td>
</tr>
</tbody>
</table>

MIB Objects

alaFcVsanTable
  alaFcVsanNumber
  alaFcVsanDescription,
  alaFcVsAnAdmStatus
  alaFcVsAnOperStatus
fibre-channel port mode

Configures the port type and operational mode for an eligible FC port. The port type is only set to Fibre Channel and the specified operational mode determines the type of gateway functionality provided on that port. There are three modes supported: N_Port proxy, F_Port proxy, and E_Port proxy.

```
fibre-channel port chassis/slot/port[-port2] mode {np | f | te} [bb-sc-n buffer_num]
```

```
no fibre-channel port chassis/slot/port[-port2]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8). Only ports on an OmniSwitch 6900 OS-XNI-U12E module with an SFP-FC-SR transceiver are eligible for this command.
- `np` Activates N_Port proxy functionality on the port. In this mode the port serves as a proxy node port (NP_Port) that aggregates N_Port transactions between FCoE devices and FC switches.
- `f` Activates F_Port proxy functionality on the port. In this mode the port operates as a fabric port (F_Port), which connects to an N_Port in a point-to-point link between FC devices.
- `te` Activates E_Port functionality on the port. In this mode, the port operates as a tunnel expansion port (TE_Port) that connects to an E_Port on an FC switch. TE_Ports allow E_Ports to connect across an FCoE network as part of an inter-switch link (ISL) tunnel that is used to expand the native FC fabric over Ethernet.
- `buffer_num` The buffer-to-buffer state change (BB_SC) number. FC ports exchange BB_SC primitives after 2^BB_SC_N frames. These primitives are used to recalculate buffer credits as part of a buffer-to-buffer flow control function between FC switch connections. The valid range is 0–15.

**Defaults**

By default, no operational mode is configured for the FC ports and the port type is set to Ethernet.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bb-sc-n buffer_num</td>
<td>0</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- Use the `no` form of this command to remove the operational mode configuration from the FC port. The port type reverts back to Ethernet.

- To change the FC mode for the port, use the `no` form of this command to remove the current mode configuration then configure the FC mode again for the same port.

- Changing the `bb-sc-n` parameter value can be changed at any time (removing the FC mode configuration is not required to change this parameter value).

- Make sure the `bb-sc-n` parameter value is the same on both ends of the connection between the OmniSwitch FCoE/FC gateway and an FC switch. If the value is different on each end of the connection then the greater value is used. However, if this value is set to zero for one of the ports on the connection, then the buffer-to-buffer state change function is disabled.

- FC ports do not participate in Ethernet features, such as a link aggregates, a virtual fabric links (VFLs) in virtual chassis (VC) configurations, standard VLANs, or FCoE VLANs.

- To ensure end-to-end lossless connectivity through the gateway switch, assign a PAUSE-enabled DCB profile to each FC port. For more information, see Chapter 5, “Configuring an FCoE Gateway”, in the *OmniSwitch AOS Release 8 Data Center Switching Guide*.

**Examples**

```
-> fibre-channel port 2/1 mode np
-> fibre-channel port 2/3 mode f
-> fibre-channel port 2/5 mode te
-> no fibre-channel port 2/5
```

To change the FC port mode:

```
-> no fibre-channel port 2/1
-> fibre-channel port 2/1 f
```

To change the `bb-sc-n` parameter value:

```
-> fibre-channel port 2/1 bb-sc-n 3
```

**Release History**

Release 7.3.3; command introduced.

**Related Commands**

- `fibre-channel vsan members` Assigns FC ports to VSANs.
- `show fibre-channel port` Displays the FC port configuration for the switch.

**MIB Objects**

- `alaFcIntfTable`
  - `alaFcIntfIfIndex`
  - `alaFcIntfMode`
  - `alaFcIntfBbScN`
  - `alaFcIntfBbCredit`
  - `alaFcIntfBbRxDataField`
  - `alaFcIntfClassOfService`
  - `alaFcIntfRowStatus`
**fibre-channel vsan members**

Configures the VSAN assignment for the specified FC port.

```
fibre-channel vsan vsan_id members port chassis/slot/port[-port2]
no fibre-channel vsan vsan_id members port chassis/slot/port[-port2]
```

**Syntax Definitions**

- `vsan_id` An existing VSAN ID number.
- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

**Defaults**

By default, all FC ports are assigned to VSAN 1.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the association between the specified FC port and VSAN.
- When an NP_Port is removed from a VSAN, a FIP CVL is generated for all the VN_Ports that are logged in through that NP_Port and an FC LOGO is sent on the FC port. An FC LOGO is also sent for any R-NPIV sessions that exist when the CVL is generated.
- When an F_Port (used for R-NPIV) is removed from a VSAN, then FC LOGO is sent to the host and also to the FCF.
- When an FC port is moved from VSAN 1 to another VSAN, traffic loss will occur for all existing sessions. Moving FC ports between other VSANs (for example, between VSAN 2 and 3) is not allowed.
- Multiple FC ports can belong to the same VSAN, but an FC port can belong to only one VSAN. In other words, it is not possible to tag FC ports with multiple VSANs.
• When a VSAN is mapped to an FCoE VLAN and an active FC port is assigned to that VSAN, the FC mode configured for that port determines the FCoE/FC gateway functionality provided. For example, if the FC port mode is set to operate as:
  – an NP_Port, then NPIV proxy functionality is automatically enabled.
  – an F_Port, then the R-NPIV functionality is automatically enabled.
  – a TE_Port and an FCoE port is set to operate as a virtual E_Port (VE_Port), then E2E tunneling functionality is automatically enabled.

• When more than one NP_Ports is associated with the same VSAN, the OmniSwitch will load balance ENode FLOGI requests across the NP_Ports for that VSAN. By default, the NP_Ports with the lowest number of logins provided is selected. If all the NP_Ports have the same number of logins provided, then the switch will select a port using a round robin algorithm.

Examples

-> fibre-channel vsan 10 members port 2/1
-> fibre-channel vsan 10 members port 2/1-3
-> no fibre-channel vsan 10 members port 2/1-3

Release History

Release 7.3.3; command introduced.

Related Commands

fibre-channel vsan
Creates an FC VSAN.
fibre-channel port mode
Configures the operational mode for the FC port.
fibre-channel npiv-proxy load-balance
Configures the load balancing method applied when more than one FC port is assigned to the same VSAN.
show fibre-channel vsan
Displays the VSAN configuration for the switch.
show fibre-channel vsan members
Displays the VSAN port assignments.

MIB Objects

alaFcVfpaTable
   alaFcVfpaVsanNumber
   alaFcVfpaIfIndex
   alaFcVfpaRowStatus
**fcoe vsan-map**

Maps an FC VSAN to an FCoE VLAN. This mapping is required to activate the processing of specific FCoE ENode traffic traveling to and from the designated virtual FC fabric through the FCoE/FC gateway OmniSwitch.

```plaintext
fcoe vsan-map vsan vsan_id vlan vlan_id
no fcoe vsan-map vsan vsan_id vlan vlan_id
```

### Syntax Definitions

- `vsan_id`  
  An existing VSAN ID number.

- `vlan_id`  
  An existing FCoE VLAN ID number.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to remove the VSAN-to-FCoE VLAN mapping.
- When a mapping is removed, all sessions associated with the FCoE VLAN are cleared.
- Only one VSAN is mapped to one FCoE VLAN.
- The FCoE/FC gateway does not participate in FCoE discovery mechanisms for FCoE VLANs not mapped to a VSAN.
- If an FCoE VLAN is not mapped to a VSAN, then only FIP snooping functionality is applied to that VLAN.

### Examples

- `fcoe vsan-map vsan 10 vlan 100`
- `no fcoe vsan-map vsan 10 vlan 100`

### Release History

Release 7.3.3; command introduced.
Related Commands

- `fibre-channel vsan` Configures a VSAN for the switch.
- `fcoe vlan` Configures an FCoE VLAN for the switch.
- `show fcoe vsan-map` Displays the VSAN-VLAN mapping configuration.

MIB Objects

- `alaFipsVsanVlanMapTable`
  - `alaFipsVsanVlanMapVsanNumber`
  - `alaFipsVsanVlanMapVlanNumber`
  - `alaFipsVsanVlanMapRowStatus`
fibre-channel npiv-proxy load-balance

Configures the dynamic load balancing method that is applied to ENode FLOGI requests when more than one FC port is associated with the same VSAN. Load balancing is not applied to FDISC requests.

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Selects the default load balancing method.</td>
</tr>
<tr>
<td><code>dynamic-reorder</code></td>
<td>Ensures that all sessions are load balanced evenly at any given time.</td>
</tr>
<tr>
<td><code>enode-based</code></td>
<td>Selects the FC for the new session based on the ENode MAC address.</td>
</tr>
</tbody>
</table>

Defaults

By default, the FC port with the lowest number of logins provided is selected for new FLOGI requests. If all the ports have the same number of logins provided, then the switch will select a port using a round robin algorithm.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The load balancing method is globally applied to the switch, and only one method is applied at a time.
- Using the dynamic reorder load balancing method may trigger the tearing down of some sessions, so that upon re-login the ENode FLOGI is processed on a different NP_Port in the same VSAN. For example, when a new FC NP_Port is added to the VSAN, some of the sessions are torn down and logged in again on the newly added port to distribute sessions across all ports in the VSAN.
- When the ENode-based load balancing method is used, each NP_Port in the VSAN will send a multicast discovery advertisement to all ENodes in the mapped FCoE VLAN. The FCF MAC address in the discovery advertisement is the MAC address of the FC port. The ENode then decides which FCF (NP_Port) to use for the login.
- The default and ENode-based load balancing methods do not disturb existing sessions.
- The load balancing method is **not** applied to statically mapped FCoE and FC ports.

Examples

- `-> fibre-channel npiv-proxy load-balance dynamic-reorder`
- `-> fibre-channel npiv-proxy load-balance enode-based`
- `-> fibre-channel npiv-proxy load-balance default`
**Release History**

Release 7.3.3; command introduced.

**Related Commands**

`fibre-channel npiv-proxy load-balance static` Configures a static mapping between an FCoE port and an FC NP_Port. Load balancing does not apply to statically mapped ports.

`show fibre-channel` Displays the global load balancing method applied to NP_Ports.

**MIB Objects**

- `alaFcInfo`  
- `alaFcConfigNpivLoadBalance`
**fibre-channel npiv-proxy load-balance static**

Configures a static port association between an FCoE port and an FC NP_Port to ensure that FC sessions on the specified FCoE port are mapped to the specified NP_Port.

`fibre-channel npiv-proxy load-balance static {port chassis/slot/port | linkagg agg_id} fc-port chassis/slot/port`

`no fibre-channel npiv-proxy load-balance static {port chassis/slot/port | linkagg agg_id} fc-port chassis/slot/port`

**Syntax Definitions**

- `chassis` The chassis identifier.
- `port slot/port` The slot and port number (3/1) of an FCoE port.
- `agg_id` The link aggregate ID number.
- `fc-port slot/port` The slot and port number (3/1) of an FC port.

**Defaults**

By default, there are no static FCoE-to-FC port associations. The dynamic load balancing method is applied to the FC NP_ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the static association between the FCoE port and the FC port. When this association is removed, the dynamic load balancing method is applied.
- Use caution when configuring static FCoE-to-FC port assignments. Static assignments exempt both the FCoE port and the FC NP_Port from dynamic load balancing of sessions when multiple FC ports belong to the same VSAN.

**Examples**

- `-> fibre-channel npiv-proxy load-balance static port 1/1 fc-port 2/1`
- `-> no fibre-channel npiv-proxy load-balance static port 1/1 fc-port 2/1`
- `-> fibre-channel npiv-proxy load-balance static linkagg 10 fc-port 2/1`
- `-> no fibre-channel npiv-proxy load-balance static linkagg 10 fc-port 2/1`
Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel npiv-proxy load-balance  
Displays the static FCoE port/FC NP_Port mapping and FC port session counts.

MIB Objects

alaFcNpivStaticLoadBalanceTable
   alaFcNpivStaticLoadBalanceRowStatus
   alaFcNpivStaticLoadBalanceEtherIfIndex
   alaFcNpivStaticLoadBalanceFibreIfIndex
fcoe e-tunnel

Configures an E2E tunnel identifier and associates the identifier with tunnel endpoints and an FCoE VLAN. An E2E tunnel allows FC switches to set up ISLs between fabrics over an FCoE network.

fcoe e-tunnel tunnel_id {fc-port1 chassis/slot/port} {fc-port2 chassis/slot/port | vlan vlan_id}
no fcoe e-tunnel tunnel_id

Syntax Definitions

tunnel_id
chassis
slot/port
vlan_id
A unique ID number to assign to this tunnel session.
The chassis identifier.
The slot and port number (3/1) of an FC tunnel edge (TE) port.
An existing FCoE VLAN ID number.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the tunnel configuration.
- An OmniSwitch FC port is configured as a tunnel E_Port (TE Port) and connects to an E_Port on an FC switch. TE_Ports can carry traffic from multiple VSANs. This command is used to associate the TE port with an FCoE VLAN or with another TE port on the same switch.
- An OmniSwitch FCoE port is configured as a virtual expansion port (VE_Port) on the FCoE network side. The VE port is associated with an FCoE VLAN by tagging the VE port with the FCoE VLAN ID.
- This command does not establish a connection. Once the required tunnel components are configured, successful exchange of exchange link parameters (ELP) between a TE_Port and a VE_Port or between two TE_Ports will establish the tunnel session.
- To create a tunnel connection between two FC switches across the FCoE network requires the following steps:
  - Configure the FCoE port that will connect to the FCoE network as a virtual expansion port
To tag the VE_Port to the FCoE VLAN that will carry traffic through the tunnel.

- Configure the FC port that will connect to an E_Port on an FC as a TE_Port.
- Use this command (fcoe e-tunnel) with the fc-port1 and vlan parameters to associate the TE_Port with the FCoE VLAN to which the VE_Port is tagged.

- To create a tunnel between two FC TE_Ports on the same switch or in a virtual chassis configuration, use the fc-port1 and fc-port2 parameters to specify the slot and port number of the two TE ports.

**Examples**

- `fcoe e-tunnel 1 fc-port1 2/1 fc-port2 2/2`
- `fcoe e-tunnel 10 fc-port1 2/3 vlan 200`
- `fcoe e-tunnel 11 fc-port1 2/4 vlan 200`
- `no fcoe e-tunnel 10`

**Release History**

Release 7.3.3; command introduced.

**Related Commands**

- `fcoe vlan`: Configures an FCoE VLAN.
- `fcoe role`: Configures an FCoE port as a VE_Port.
- `fibre-channel port mode`: Configures an FC port as a TE_Port
- `show fcoe e-tunnel`: Displays the E2E tunnel configuration.
- `show fibre-channel sessions`: Displays FC sessions on FC ports.

**MIB Objects**

- `alaFipsEtunnelTable`
- `alaFipsEtunnelVlanId`
- `alaFipsEtunnelIfIndexOne`
- `alaFipsEtunnelIfIndexTwo`
- `alaFipsEtunnelRowStatus`
show fibre-channel vsan

Displays the VSAN configuration for the switch.

`show fibre-channel vsan [vsan_id][vsan_id2]`

**Syntax Definitions**

| vsan_id[vsan_id2] | An existing VSAN ID. Use a hyphen to specify a range of VSAN IDs (10-25). |

**Defaults**

By default, a list of all VSANs is displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify a VSAN ID with this command to display information about a specific VSAN.

**Examples**

```
-> show fibre-channel vsan

vsan  oper  admin  name
-------+----+-----+---------
   1   Ena  Dis  test1
  1000 Dis  Dis  test2
  2000 Ena  Dis  test3

-> show fibre-channel vsan 101

vsan  oper  admin  name
-------+----+-----+---------
  1000 Dis  Dis  test2

output definitions:

<table>
<thead>
<tr>
<th>vsan</th>
<th>The numerical VSAN ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>oper</td>
<td>The operational status of the VSAN: <strong>Ena</strong> (enabled) or <strong>Dis</strong> (disabled). The operational status remains disabled until an active FC port is assigned to the VSAN. A VSAN must have an enabled administrative status before it can become operationally enabled.</td>
</tr>
</tbody>
</table>
**output definitions (continued)**

<table>
<thead>
<tr>
<th>admin</th>
<th>The administrative status of the VSAN: <strong>Ena</strong> specifies that VSAN functions are enabled; <strong>Dis</strong> specifies that VLAN functions are disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The user-defined text description for the VSAN. By default, the VSAN ID is displayed if the VLAN description is not specified.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command introduced.

**Related Commands**

- **fibre-channel vsan** Configures a VSAN for the switch.
- **show fibre-channel vsan members** Displays VSAN port assignments.

**MIB Objects**

- **alaFcVsanTable**
  - **alaFcVsanNumber**
  - **alaFcVsanDescription**
  - **alaFcVsanAdmStatus**
  - **alaFcVsanOperStatus**
  - **alaFcVsanRowStatus**
**show fibre-channel vsan members**

Displays the VSAN port assignments.

```
show fibre-channel vsan [vsan_id [-vsan_id2]] members [port chassis/slot/port[-port2]]
```

### Syntax Definitions

- **vsan_id[[-vsan_id2]]**  
  An existing VSAN ID number. Use a hyphen to specify a range of VSAN IDs (10-25).

- **chassis**  
  The chassis identifier.

- **slot/port[[-port2]]**  
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

### Defaults

By default, all VSAN port assignments are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C4E/N48C8/</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 C32E/T24C2/</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900 X24C2</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If the **vsan_id** is specified without a **slot/port**, then all port assignments for that VSAN are displayed.
- If both the **vsan_id** and **slot/port** are specified, then information only for that VSAN and slot/port is displayed.
- Only OmniSwitch FC ports can be assigned to a VSAN.

### Examples

```
-> show fibre-channel vsan members
vsan port status
----------
1  2/2/1 Enabled
1003  2/2/12 Enabled
1005  3/2/5 Disabled

-> show fibre-channel vsan 1003 members
port status
-------------
2/2/12  Enabled

-> show fibre-channel vsan 1005 members port 3/2/5
vsan : 1005,
port : 3/2/5,
status : disabled
```
show fibre-channel vsan members

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsan</td>
<td>The numerical VSAN ID. Configured through the <code>fibre-channel vsan</code> command.</td>
</tr>
<tr>
<td>port</td>
<td>The FC port number associated with the VSAN ID. Configured through the <code>fibre-channel vsan members</code> command.</td>
</tr>
<tr>
<td>status</td>
<td>The operational status of the port (enabled or disabled).</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command introduced.

Related Commands

show fibre-channel vsan  Displays the VSAN configuration for the switch.

MIB Objects

alaFcVfpaTable
  alaFcVfpaVsanNumber
  alaFcVfpaIfIndex
  alaFcVfpaState
  alaFcVfpaRowStatus
show fibre-channel port

Displays the FC port configuration for the switch.

show fibre-channel port [info]

**Syntax Definitions**

info Displays session details for each FC port.

**Defaults**

By default, the parameters for each FC port are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the *info* parameter is used with this command, the *fcid* field shows an FC port ID for NP_Ports. For all other port modes, this field is blank. Only NP_Ports perform fabric login (FLOGI) and obtain a port ID from an FC switch.
- If an FC port is configured to operate in the fabric or tunnel E_Port mode, there is no fabric login process performed. Ports running in these modes will come up immediately.
- FLOGI is triggered only after an NP_Port is assigned to a VSAN.

**Examples**

```
-> show fibre-channel port
Legend: NP=Proxy N_Port, F=Fabric Port connected to N_port, TE=Tunnel E-Port

ports oper-status mode  BB-SC-N  service class
---------------+----------+---------------+-------------+-----------+-------------+-------------+-------------+-----------+-------------+-------------+-----------
 2/1        Up      NP        3              3
 2/2        Up      F         0              3
 2/3        Up      TE        3              3/F
 2/4       Down     NP        0              3
```

**output definitions**

- **ports** The slot and port number of the FC port.
- **oper-status** The operational status of the FC port.
The operational mode for the FC port.

The buffer-to-buffer state change number configured for the FC port.

The service class for the FC port session (2, 3, F, or 3/F). This value indicates the level of delivery integrity required for an application.

Legend: NP=Proxy N_Port, F=Fabric Port connected to N_port, TE=Tunnel E_Port

<table>
<thead>
<tr>
<th>ports</th>
<th>mode</th>
<th>fcid</th>
<th>wwpn</th>
<th>state</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>NP</td>
<td>010010c</td>
<td>10:00:01:00:00:0a:22:11</td>
<td>Up</td>
</tr>
<tr>
<td>2/2</td>
<td>F</td>
<td>-</td>
<td>10:00:01:00:00:0b:22:1a</td>
<td>Up</td>
</tr>
<tr>
<td>2/3</td>
<td>TE</td>
<td>-</td>
<td>10:00:01:00:00:0b:23:22</td>
<td>Up</td>
</tr>
<tr>
<td>2/4</td>
<td>NP</td>
<td>-</td>
<td>10:00:01:00:00:0b:23:23</td>
<td>FLOGI_Sent</td>
</tr>
<tr>
<td>2/5</td>
<td>NP</td>
<td>-</td>
<td>10:00:01:00:00:0b:23:24</td>
<td>Not_Init</td>
</tr>
</tbody>
</table>

The slot and port number of the FC port.
The operational mode for the FC port (NP = proxy N_Port, F = fabric port, TE = tunnel E_Port). Configured through the fibre-channel port command.

The FC port_ID obtained after successful fabric login. This field applies only to NP_Ports.
The world-wide port name assigned to the OmniSwitch FC port.
The operational state of the fabric login process (Up, Down, FLOGI_Sent, Not_Init, ELP_Sent, Sess_Clear).

Release 7.3.3; command introduced.

show fibre-channel vsan
Displays the VSAN configuration for the switch.
show fibre-channel vsan members
Displays the VSAN port assignments for the switch.

alaFcIntfTable
alaFcIntfIfIndex
alaFcIntfOperStatus
alaFcIntfMode
alaFcIntfBbScN
alaFcIntfBbCredit
alaFcIntfBbRxDataField
alaFcIntfClassOfService
alaFcIntfFcid
alaFcIntfWwpn
alaFcIntfLoginState
alaFcIntfRowStatus
**show fcoe vsan-map**

Displays the VSAN-to-FCoE VLAN mapping configuration.

```
show fcoe vsan-map
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>vsan</th>
<th>vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>2000</td>
<td>2000</td>
</tr>
<tr>
<td>3000</td>
<td>3000</td>
</tr>
</tbody>
</table>

#### Defaults

N/A

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

Mapping a VSAN to an FCoE VLAN is required to activate the processing of specific ENode traffic traveling to and from the designated virtual FC fabric through the NPIV OmniSwitch.

#### Examples

```
-> show fcoe vsan-map
vsan  vlan
------- -------
   10     10
   2000   2000
   3000   3000
```

#### Output Definitions

<table>
<thead>
<tr>
<th>vsan</th>
<th>vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>The VSAN ID. Configured through the <code>fibre-channel vsan</code> command.</td>
<td></td>
</tr>
<tr>
<td>The FCoE VLAN ID. Configured through the <code>fcoe vlan</code> command.</td>
<td></td>
</tr>
</tbody>
</table>

#### Release History

Release 7.3.3; command introduced.
Related Commands

**fcoe vsan-map**
Configures a one-to-one mapping between a VSAN and FCoE VLAN.

**show vlan**
Displays the FCoE VLAN configuration.

MIB Objects

alaFipsVsanVlanMapTable

alaFipsVsanVlanMapVsNumber
alaFipsVsanVlanMapVlanNumber
alaFipsVsanVlanMapRowStatus
show fibre-channel sessions

Displays the sessions established on the OmniSwitch FC ports.

**show fibre-channel sessions [vsan vsan_id | e-tunnel tunnel_id] [port chassis/slot/port] [summary]**

### Syntax Definitions

- **vsan_id**: An existing VSAN ID number.
- **tunnel_id**: An existing E-Tunnel (E2E Tunnel) ID.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1).

### Defaults

By default, all FC sessions are displayed for all FC ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **port** parameter can be combined with the **vsan** or **e-tunnel** parameters to display sessions for a specific FC port within a VSAN or E2E tunnel.

### Examples

- `-> show fibre-channel sessions summary`
  
  Total FIBRE-CHANNEL Sessions: 7 ,
  Total NPIV Sessions: 4 ,
  Total R-NPIV Sessions: 1 ,
  Total E-TUNNEL Sessions: 2

- `-> show fibre-channel sessions`
  
  Total FIBRE-CHANNEL Sessions: 4
  Total NPIV Sessions: 2
  Total R-NPIV Sessions: 1
  Total E-TUNNEL Sessions: 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>VSAN</th>
<th>T-ID</th>
<th>WWPN</th>
<th>FCID</th>
<th>Status</th>
<th>Login Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/1</td>
<td>NP</td>
<td>100</td>
<td>-</td>
<td>11:00:00:17:A4:B1:71:23</td>
<td>00:01:01</td>
<td>SUCCESS</td>
<td>FLOGI</td>
</tr>
<tr>
<td>2/2</td>
<td>P</td>
<td>200</td>
<td>-</td>
<td>11:00:00:17:A4:B1:72:24</td>
<td>00:01:02</td>
<td>SUCCESS</td>
<td>FLOGI</td>
</tr>
<tr>
<td>2/1</td>
<td>NP</td>
<td>100</td>
<td>-</td>
<td>11:00:00:17:A4:B1:71:24</td>
<td>00:01:03</td>
<td>SUCCESS</td>
<td>FDISC</td>
</tr>
</tbody>
</table>
FCoE/FC Gateway Commands

show fibre-channel sessions

```
2/3 TE - 11:00:00:17:A4:B1:71:2a - SUCCESS ELP

-> show fibre-channel sessions vsan 200
Port Mode VSAN T-ID WWPN FCID Status Login Type
--------+----+----+----+-----------------------+--------+--------+-------------
2/2 F 200 - 11:00:00:17:A4:B1:72:24 00:01:02 SUCCESS FLOGI

-> show fibre-channel sessions port 2/1
Port Mode VSAN T-ID WWPN FCID Status Login Type
--------+----+----+----+-----------------------+--------+--------+-------------
2/1 NP 100 - 11:00:00:17:A4:B1:71:23 00:01:01 SUCCESS FLOGI
2/1 NP 100 - 11:00:00:17:A4:B1:71:24 00:01:03 SUCCESS FDISC

-> show fibre-channel sessions e-tunnel 10
Port Mode VSAN T-ID WWPN FCID Status Login Type
--------+----+----+----+-----------------------+--------+--------+-------------
2/3 TE - 10 11:00:00:17:A4:B1:71:2a - SUCCESS ELP
2/4 TE - 10 11:00:00:17:A4:B1:71:2b - SUCCESS ELP

-> show fibre-channel sessions e-tunnel 10 port 2/3
Port Mode VSAN T-ID WWPN FCID Status Login Type
--------+----+----+----+-----------------------+--------+--------+-------------
2/3 TE - 10 11:00:00:17:A4:B1:71:2a - SUCCESS ELP

-> show fibre-channel sessions port 2/3
Port Mode VSAN T-ID WWPN FCID Status Login Type
--------+----+----+----+-----------------------+--------+--------+-------------
2/3 TE - 10 11:00:00:17:A4:B1:71:2a - SUCCESS ELP
```

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The slot and port number for the FC port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>The operational mode for the FC port (F = F_Port, NP = proxy N_Port, TE = tunnel E_Port). Configured through the fibre-channel port mode.</td>
</tr>
<tr>
<td>vsan</td>
<td>The VSAN ID to which the NP_Port or F_Port is assigned. Configured through the fibre-channel vsan command.</td>
</tr>
<tr>
<td>T-ID</td>
<td>The E2E tunnel ID. Configured through the fcoe e-tunnel command.</td>
</tr>
<tr>
<td>WWPN</td>
<td>The world-wide port name associated with the OmniSwitch FC port.</td>
</tr>
<tr>
<td>FCID</td>
<td>The FC port ID assigned to the node during login.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the login session.</td>
</tr>
<tr>
<td>Login Type</td>
<td>The type of login (FLOGI = fabric login, FDISC = fabric discovery, or ELP = exchange link parameters).</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command introduced.
Related Commands

- **clear fibre-channel sessions**
  - Clears FC sessions.
- **show fibre-channel node**
  - Displays a list of FC nodes connected through the switch.

MIB Objects

alaFcSessTable
  - alaFcSessIfIndex
  - alaFcSessVsanNumber,
  - alaFcSessStatus,
  - alaFcSessIntfMode,
  - alaFcSessFcid,
  - alaFcSessWwpn,
  - alaFcSessType,
  - alaFcSessTunnelId
show fibre-channel node

Displays a list of FC nodes connected to OmniSwitch FC ports.

show fibre-channel node [vsan vsan_id | port chassis/slot/port]

Syntax Definitions

- **vsan_id**: An existing VSAN ID number.
- **chassis**: The chassis identifier.
- **slot/port**: The slot and port number (3/1).

Defaults

By default, a list of all FC nodes is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specify a VSAN ID to display nodes associated with a specific VSAN.
- Specify an FC port number to display nodes connected on a specific FC port.

Examples

```
-> show fibre-channel node
VSAN  VLAN  WWNN                     WWPN              Port   FC-ID
-----+-----+-----------------------+-----------------------+------+--------
 1    200  20:00:00:24:FF:37:DD:BB 21:00:00:24:FF:37:DD:BB  2/7   02:09:02
10   100  11:00:00:17:A4:B1:71:23 11:00:00:17:A4:B1:71:23  2/1   00:0A:01
10    -   11:00:00:17:A4:B1:71:24 11:00:00:17:A4:B1:71:24  2/2   00:0B:02

-> show fibre-channel node vsan 10
VSAN  VLAN  WWNN                WWPN                   Port    FC-ID
-----+-----+------------------------+-----------------------+-------------
10    100  11:00:00:17:A4:B1:71:23  11:00:00:17:A4:B1:71:23  2/1  00:0A:01
10     -   11:00:00:17:A4:B1:71:24  11:00:00:17:A4:B1:71:24  2/2  00:0B:02

-> show fibre-channel node port 2/1
Port  VSAN  VLAN  WWNN                WWPN                   FC-ID
-----+-----+-----+------------------------+-----------------------+-------
 2/1  10   100 11:00:00:17:A4:B1:71:23 11:00:00:17:A4:B1:71:23  00:0A:01
```
**output definitions**

<table>
<thead>
<tr>
<th>Port</th>
<th>The slot/port of the FC interface that is connected to the FC node.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSAN</td>
<td>The VSAN ID associated with the FC node. Configured through the <strong>fibre-channel vsan</strong> command.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The FCoE VLAN ID on which FC nodes are provided. Configured through the <strong>fcoe vlan</strong> command.</td>
</tr>
<tr>
<td>WWNN</td>
<td>The world-wide node name assigned to an FC node.</td>
</tr>
<tr>
<td>WWPN</td>
<td>The world-wide port name assigned to the FC port.</td>
</tr>
<tr>
<td>FC-ID</td>
<td>The FC port ID assigned to an N_Port (or VN_Port, or NP_Port) after successful fabric login.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command introduced.

**Related Commands**

- **show fibre-channel sessions** Displays the sessions established on the OmniSwitch FC ports.

**MIB Objects**

alaFcNodeTable
- alaFcNodeIfIndex
- alaFcNodeVsanNumber
- alaFcNodeVlanNumber
- alaFcNodeFcId
- alaFcNodeWwpn
- alaFcNodeWwnn
**show fcoe e-tunnel**

Displays the E2E tunnel configuration for the switch.

```
show fcoe e-tunnel [tunnel_id]
```

## Syntax Definitions

- **tunnel_id**: An existing tunnel ID number.

## Defaults

N/A

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Use the `tunnel_id` to display parameters for a specific tunnel.

## Examples

```
-> show fcoe e-tunnel

tunnel  vlan  Port1   Port2
-------+-----+-------+----------
 1   1000  1/1/1     -
 2     -   1/1/2   3/3/1
 3   3000  1/1/3     -

-> show fcoe e-tunnel 2

tunnel  vlan  Port1   Port2
-------+-----+-------+----------
 2     -   1/1/2   3/3/1
```

## Output Definitions

- **Tunnel**: The E2E tunnel ID associated with the session. Configured through
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan</td>
<td>The FCoE VLAN on which the tunnel is defined. Configured through the <code>fcoe vlan</code> command.</td>
</tr>
<tr>
<td>Port1, Port2</td>
<td>The FCoE port (in VE_Port role) and/or FC port (in TE_Port mode) for this session. The FCoE port rule is configured through the <code>fcoe role</code> command. The FC port mode is configured through the <code>fibre-channel port mode</code> command.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command introduced.

**Related Commands**

`fcoe e-tunnel` Configures E2E tunnel parameters.

**MIB Objects**

`alaFipsEtunnelTable`
- `alaFipsEtunnelId`
- `alaFipsEtunnelVlanId`
- `alaFipsEtunnelIfIndexOne`
- `alaFipsEtunnelIfIndexTwo`
show fibre-channel

Displays global Fibre Channel parameter values.

show fibre-channel

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 7.3.3</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command currently displays the following:

- The load-balancing method that is applied to FLOGI requests when there is more than one NPIV proxy port assigned to the same VSAN. This mode does not apply to FC ports configured to operate in the F_Portal proxy mode (R-NPIV) or as E2E tunnel ports.
- The World Wide Node Name (WWNN) for the switch. The WWNN is comprised of “10:00” combined with the next available increment of the switch based MAC address.

Examples

-> show fibre-channel
Fibre Channel Global Configurations :
----------------------------------------
NPIV Proxy Global Load Balance Method : Default
Local WWNN : 10:00:00:E0:B1:E7:09:A4

Release History

Release 7.3.3; command introduced.
Related Commands

`fibre-channel npiv-proxy load-balance` Configures the load balancing method applied to multiple FC ports that belong to the same VSAN.

MIB Objects

`alaFipsEtunnelTable`
- `alaFipsEtunnelId`
- `alaFipsEtunnelVlanId`
- `alaFipsEtunnelIfIndexOne`
- `alaFipsEtunnelIfIndexTwo`
show fibre-channel statistics

Displays FC port statistics.

```
show fibre-channel statistics [npiv | r-npiv] [vsan vsan_id[vsan_id2]] [port chassis/slot/port[-port2]] [e-tunnel port chassis/slot/port[-port2]]
```

### Syntax Definitions

- **npiv**: Displays statistics for N_Port proxy sessions.
- **r-npiv**: Displays statistics for F_Port proxy sessions.
- **e-tunnel [tunnel_id]**: Displays E2E tunnel (E_Port proxy) statistics. Optionally enter a tunnel ID to display information for a specific tunnel.
- **vsan_id[vsan_id2]**: An existing VSAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VSAN IDs (100-150).
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

### Defaults

By default, all statistics are displayed

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **vsan** parameter to display statistics for a specific VSAN ID. The **vsan** parameter is not used with the **e-tunnel** parameter, because tunnel ports are not associated with a VSAN.
- Use the **port** parameter to display statistics for a specific FC port.
**Examples**

-> show fibre-channel statistics vsan 46

**NPIV VSAN Statistics:**

<table>
<thead>
<tr>
<th>VSAN</th>
<th>LS_ACC</th>
<th>FLOGO</th>
<th>LS_RJT</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>29</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>VSAN</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>FLOGO</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>5</td>
<td>18</td>
<td>14</td>
</tr>
</tbody>
</table>

**R-NPIV VSAN Statistics:**

**Packets Received:**

<table>
<thead>
<tr>
<th>VSAN</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>FLOGO</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>VSAN</th>
<th>FLOGI_ACC</th>
<th>FLOGI_RJT</th>
<th>FDISC_ACC</th>
<th>FDISC_RJT</th>
<th>FLOGO</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

-> show fibre-channel statistics npiv vsan 46

**NPIV VSAN Statistics:**

**Packets Received:**

<table>
<thead>
<tr>
<th>VSAN</th>
<th>LS_ACC</th>
<th>FLOGO</th>
<th>LS_RJT</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>29</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>VSAN</th>
<th>FLOGI</th>
<th>FDISC</th>
<th>FLOGO</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>5</td>
<td>18</td>
<td>14</td>
</tr>
</tbody>
</table>

-> show fibre-channel statistics e-tunnel port 1/2/3

**E-Tunnel Port Statistics**

**Packets Received:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Tunnel</th>
<th>ELP</th>
<th>SW_ACC</th>
<th>SW_RJT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2/3</td>
<td>2</td>
<td>3</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

**Packets Sent:**

<table>
<thead>
<tr>
<th>Port</th>
<th>Tunnel</th>
<th>ELP</th>
<th>SW_ACC</th>
<th>SW_RJT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2/3</td>
<td>2</td>
<td>9483</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.3; command introduced.
Related Commands

clear fibre-channel statistics  Clears FC port statistics.

MIB Objects

alaFcIntfNpivStatsTable
  alaFcIntfNpivStatsIfIndex
  alaFcIntfNpivStatsFlgiscs
  alaFcIntfNpivStatsFlgiscsLsAccs
  alaFcIntfNpivStatsFlgiscsSwRjts
  alaFcIntfNpivStatsFlgiscsSwRjts

alaFcVsanNpivStatsTable
  alaFcVsanNpivStatsVsan
  alaFcVsanNpivStatsFlgiscs
  alaFcVsanNpivStatsFlgiscsLsAccs
  alaFcVsanNpivStatsFlgiscsSwRjts
  alaFcVsanNpivStatsFlgiscsSwRjts

alaFcIntfRnpivStatsTable
  alaFcIntfRnpivStatsIfIndex
  alaFcIntfRnpivStatsFlgiscs
  alaFcIntfRnpivStatsFlgiscsLsAccs
  alaFcIntfRnpivStatsFlgiscsSwRjts
  alaFcIntfRnpivStatsFlgiscsSwRjts

alaFcVsanRnpivStatsTable
  alaFcVsanRnpivStatsVsan
  alaFcVsanRnpivStatsFlgiscs
  alaFcVsanRnpivStatsFlgiscsLsAccs
  alaFcVsanRnpivStatsFlgiscsSwRjts
  alaFcVsanRnpivStatsFlgiscsSwRjts

alaFcTidEtunnelStatsTable
  alaFcTidEtunnelStatsTunnelId
  alaFcTidEtunnelStatsElpReqs
  alaFcTidEtunnelStatsSwAccs
  alaFcTidEtunnelStatsSwRjts

alaFcIntfEtunnelStatsTable
  alaFcIntfEtunnelStatsIfIndex
  alaFcIntfEtunnelStatsElpReqs
  alaFcIntfEtunnelStatsSwAccs
  alaFcIntfEtunnelStatsSwRjts

alaFcTidEtunnelStatsTable
  alaFcTidEtunnelStatsTunnelId
  alaFcTidEtunnelStatsElpReqs
  alaFcTidEtunnelStatsSwAccs
  alaFcTidEtunnelStatsSwRjts

alaFcIntfEtunnelStatsTable
  alaFcIntfEtunnelStatsIfIndex
  alaFcIntfEtunnelStatsElpReqs
  alaFcIntfEtunnelStatsSwAccs
  alaFcIntfEtunnelStatsSwRjts
show fcoe statistics npiv-proxy

Displays ENode fabric login or ENode discovery statistics for FCoE interfaces or specific VLANs.

```
show fcoe statistics npiv-proxy {enode-login | enode-discovery} {interface | vlan [vlan_id|vlan_id2] | port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- `enode-login` Displays ENode login statistics.
- `enode-discovery` Displays ENode discovery statistics.
- `interface` Display statistics for all FCoE interfaces (ports and link aggregates).
- `vlan_id[vlan_id2]` An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `vlan` parameter to display statistics for a specific FCoE VLAN ID.
- Use the `port` or `linkagg` parameters to display statistics for a specific FCoE port or link aggregate ID.

**Examples**

```
->show fcoe statistics npiv-proxy enode-discovery interface
Packets Received:
  Port   Vlan  Req   MDS   UDS
  --------+-------+-------+-------+-------+
     1/1    1   1     0
     1/22   1   1     0
Packets Sent:
  Port   Vlan   Res   MDA   UDA
  --------+-------+-------+-------+-------+
```
```
1/1            1      3         1
1/22           1      3         1

-> show fcoe statistics npiv-proxy enode-login interface
Packets Received:
    Port   FLOGI   FDISC   LOGO  E_KA  VN_KA
    -------+---------+---------+-------+-------+-------+
    1/12     0       0       0      0      0

Packets Sent:
    Port  FLOGI_ACC  FDISC_ACC  FLOGO_ACC  FLOGI_RJT  FDISC_RJT  FLOGO_RJT    CVL
    -------+-------------------------------------------+---------+---------+---------+
    1/12     0       0       0       0       0       0       0
```

**Release History**

Release 7.3.3; command introduced.

**Related Commands**

`clear fcoe statistics npiv`  
Clears ENode and FCF statistics.
**MIB Objects**

- `alaFipsVlanNpivDiscStatsTable`
  - `alaFipsVlanNpivDiscStatsVlanId`
  - `alaFipsVlanNpivDiscStatsVlanDiscRqs`
  - `alaFipsVlanNpivDiscStatsVlanDiscResps`
  - `alaFipsVlanNpivDiscStatsMdss`
  - `alaFipsVlanNpivDiscStatsUdss`
  - `alaFipsVlanNpivDiscStatsMdas`
  - `alaFipsVlanNpivDiscStatsUdas`
  - `alaFipsVlanNpivDiscStatsVnkas`

- `alaFipsIntfNpivDiscStatsTable`
  - `alaFipsIntfNpivDiscStatsIfIndex`
  - `alaFipsIntfNpivDiscStatsVlanDiscRqs`
  - `alaFipsIntfNpivDiscStatsVlanDiscResps`
  - `alaFipsIntfNpivDiscStatsMdss`
  - `alaFipsIntfNpivDiscStatsUdss`
  - `alaFipsIntfNpivDiscStatsMdas`
  - `alaFipsIntfNpivDiscStatsUdas`
  - `alaFipsIntfNpivDiscStatsVnkas`

- `alaFipsVlanNpivLoginStatsTable`
  - `alaFipsVlanNpivLoginStatsVlanId`
  - `alaFipsVlanNpivLoginStatsFlogis`
  - `alaFipsVlanNpivLoginStatsFdiscs`
  - `alaFipsVlanNpivLoginStatsLsAccs`
  - `alaFipsVlanNpivLoginStatsLsRjts`
  - `alaFipsVlanNpivLoginStatsLogos`
  - `alaFipsVlanNpivLoginStatsCvls`
  - `alaFipsVlanNpivLoginStatsEkas`
  - `alaFipsVlanNpivLoginStatsVnkas`

- `alaFipsIntfNpivLoginStatsTable`
  - `alaFipsIntfNpivLoginStatsIfIndex`
  - `alaFipsIntfNpivLoginStatsFlogis`
  - `alaFipsIntfNpivLoginStatsFdiscs`
  - `alaFipsIntfNpivLoginStatsLsAccs`
  - `alaFipsIntfNpivLoginStatsLsRjts`
  - `alaFipsIntfNpivLoginStatsLogos`
  - `alaFipsIntfNpivLoginStatsCvls`
  - `alaFipsIntfNpivLoginStatsEkas`
  - `alaFipsIntfNpivLoginStatsVnkas`
show fcoe statistics r-npiv

Displays FCF discovery fabric login or ENode discovery statistics for FCoE interfaces or specific VLANs.

show fcoe statistics r-npiv {node-login | fcf-discovery} {interface | vlan [vlan_id|vlan_id2] | port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}

Syntax Definitions

- **node-login**: Displays FC node login statistics.
- **fcf-discovery**: Displays FCF discovery statistics.
- **interface**: Display statistics for all FCoE interfaces (ports and link aggregates).
- **vlan_id[vlan_id2]**: An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults

N/A.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **vlan** parameter to display statistics for a specific FCoE VLAN ID.
- Use the **port** or **linkagg** parameters to display statistics for a specific FCoE port or link aggregate ID.

Examples

```
-> show fcoe statistics r-npiv fcf-discovery interface
Packets Received:
    Port  MDA   UDA
    --------  ------
    1/1   1     4
    1/5   8     3
Packets Sent :
    Port  MDS   UDS
    --------  ------
    1/1   1     4
```
-> show fcoe statistics r-npiv fcf-discovery linkagg 2
Packets Received:
   Port     MDA       UDA
   --------+---------+---------
0/2       3167         1
Packets Sent:
   Port     MDS       UDS
   --------+---------+---------
0/2              0         1

-> show fcoe statistics r-npiv node-login interface
Packets Received:
   Port     FLOGI_ACC  FDISC_ACC  FLOGI_RJT  FDISC_RJT  CVL
   --------+---------+---------+---------+---------+---------
0/2              3         0         0         0         0

Packets Sent:
   Port     FLOGI     FDISC     LOGO     VN-KA     E-KA
   --------+---------+---------+---------+---------+---------
0/2              3         0         0       271      3048

Release History

Release 7.3.3; command introduced.

Related Commands

**clear fcoe statistics r-npiv**  
Clears ENode and FCF statistics.
MIB Objects
alaFipsVlanRnpivDiscStatsTable
alaFipsVlanRnpivDiscStatsVlanId
alaFipsVlanRnpivDiscStatsMdss
alaFipsVlanRnpivDiscStatsUdss
alaFipsVlanRnpivDiscStatsMdss
alaFipsVlanRnpivDiscStatsUdss
alaFipsIntfRnpivDiscStatsTable
alaFipsIntfRnpivDiscStatsIfIndex
alaFipsIntfRnpivDiscStatsMdss
alaFipsIntfRnpivDiscStatsUdss
alaFipsIntfRnpivDiscStatsMdss
alaFipsIntfRnpivDiscStatsUdss
alaFipsVlanRnpivLoginStatsTable
alaFipsVlanRnpivLoginStatsVlanId
alaFipsVlanRnpivLoginStatsFlogis
alaFipsVlanRnpivLoginStatsFdiscs
alaFipsVlanRnpivLoginStatsLsAccs
alaFipsVlanRnpivLoginStatsFlogisLsRjts
alaFipsVlanRnpivLoginStatsFdiscLsRjts
alaFipsVlanRnpivLoginStatsCvls
alaFipsVlanRnpivLoginStatsLogos
alaFipsVlanRnpivLoginStatsVnkas
alaFipsVlanRnpivLoginStatsEkas
alaFipsVlanRnpivLoginStatsClear
alaFipsIntfRnpivLoginStatsTable
alaFipsIntfRnpivLoginStatsIfIndex
alaFipsIntfRnpivLoginStatsFlogis
alaFipsIntfRnpivLoginStatsFdiscs
alaFipsIntfRnpivLoginStatsLsAccs
alaFipsIntfRnpivLoginStatsFlogisLsRjts
alaFipsIntfRnpivLoginStatsFdiscLsRjts
alaFipsIntfRnpivLoginStatsCvls
alaFipsIntfRnpivLoginStatsLogos
alaFipsIntfRnpivLoginStatsVnkas
alaFipsIntfRnpivLoginStatsEkas
show fcoe statistics e-tunnel

Displays E2E tunnel statistics.

show fcoe statistics e-tunnel [ve | te] [tunnel_id|-tunnel_id]

**Syntax Definitions**

ve Displays VE_Port statistics.
te Displays TE_Port statistics.
tunnel_id[-tunnel_id] The ID of an existing E2E tunnel. Use a hyphen to specify a range of tunnel IDs (10-15).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `vlan` parameter to display statistics for a specific FCoE VLAN ID.
- Use the `port` or `linkagg` parameters to display statistics for a specific FCoE port or link aggregate ID.

**Examples**

```
-> show fcoe statistics e-tunnel

Packet Received:
Tunnel  ELP  SW_ACC  SW_RJT
---------------
15 7 1 6
17 5 4 1

Packet Sent:
Tunnel  ELP  SW_ACC  SW_RJT
---------------
15 7 1 6
17 5 4 1

Packet Received:
Tunnel  MDS  UDS  MDA  UDA  ELP_REQ  SW_ACC  SW_RJT  CVL
---------------
15 1 6 1 4 3 1 1 7
```
### FCoE/FC Gateway Commands

```
17  2  1  8  3  3  1  5  9
Packet Sent :
Tunnel  MDS  UDS  MDA  UDA  ELP_REQ  SW_ACC  SW_RJT  CVL
-----------------------------------------------
15  1  6  1  4  3  1  1  7
17  2  1  8  3  3  1  5  9
-> show fcoe statistics e-tunnel te
```

```
Packet Received :
Tunnel  ELP  SW_ACC  SW_RJT
---------------------------
15  7  1  6
17  5  4  1
Packet Sent :
Tunnel  ELP  SW_ACC  SW_RJT
---------------------------
15  7  1  6
17  5  4  1
```

```
-> show fcoe statistics e-tunnel te 17
```

```
Packet Received :
Tunnel  ELP  SW_ACC  SW_RJT
---------------------------
17  5  4  1
Packet Sent :
Tunnel  ELP  SW_ACC  SW_RJT
---------------------------
17  5  4  1
```

```
-> show fcoe statistics e-tunnel ve
```

```
Packet Received :
Tunnel  MDS  UDS  MDA  UDA  ELP_REQ  SW_ACC  SW_RJT  CVL
-----------------------------------------------
15  1  6  1  4  3  1  1  7
17  2  1  8  3  3  1  5  9
Packet Sent :
Tunnel  MDS  UDS  MDA  UDA  ELP_REQ  SW_ACC  SW_RJT  CVL
-----------------------------------------------
15  1  6  1  4  3  1  1  7
17  2  1  8  3  3  1  5  9
```

```
-> show fcoe statistics e-tunnel ve 17
```

```
Packet Received :
Tunnel  MDS  UDS  MDA  UDA  ELP_REQ  SW_ACC  SW_RJT  CVL
-----------------------------------------------
17  2  1  8  3  3  1  5  9
Packet Sent :
Tunnel  MDS  UDS  MDA  UDA  ELP_REQ  SW_ACC  SW_RJT  CVL
-----------------------------------------------
17  2  1  8  3  3  1  5  9
```

### Release History

Release 7.3.3; command introduced.
Related Commands

**clear fcoe statistics e-tunnel**  Clears ENode and FCF statistics.

MIB Objects

alaFipsEtunnelVePortStatsTable
- alaFipsEtunnelVePortStatsTunnelId
- alaFipsEtunnelVePortStatsIfIndex
- alaFipsEtunnelVePortStatsMdss
- alaFipsEtunnelVePortStatsUdss
- alaFipsEtunnelVePortStatsMdas
- alaFipsEtunnelVePortStatsUdas
- alaFipsEtunnelVePortStatsElpReqs
- alaFipsEtunnelVePortStatsSwAccs
- alaFipsEtunnelVePortStatsSwRjts
- alaFipsEtunnelVePortStatsCvls

alaFipsEtunnelTePortStatsTable
- alaFipsEtunnelTePortStatsTunnelId
- alaFipsEtunnelTePortStatsIfIndex
- alaFipsEtunnelTePortStatsElpReqs
- alaFipsEtunnelTePortStatsSwAccs
- alaFipsEtunnelTePortStatsSwRjts
show fibre-channel npiv-proxy load-balance

Displays the NPIV proxy load balancing static mapping and session count.

show fibre-channel npiv-proxy load balance {static | session-count}

Syntax Definitions

| static | Displays the static FCoE port/FC NP_Port mapping. |
| session-count | Displays the number of sessions on each FC port. |

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command displays information only for FC ports operating in the NP_Prot mode.
- Use the static parameter to display only the static mapping of FCoE ports to FC NP_Ports.
- When the session-count parameter is used, the “FC Port” field includes all NP_Ports.

Examples

- show fibre-channel npiv-proxy load-balance static

  FCoE Port   FC port
  -----------+---------
  1/1        2/1
  1/2        2/1

- show fibre-channel npiv-proxy load-balance session-count

  FC Port   session_count
  -----------+---------
  2/1       2
  2/2       0
output definitions

<table>
<thead>
<tr>
<th>FCoE Port</th>
<th>The slot/port of the FCoE port that is mapped to the FC port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC Port</td>
<td>The slot/port of the FC NP_Port.</td>
</tr>
<tr>
<td>Session Count</td>
<td>The number of sessions per FC port.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.3; command introduced.

Related Commands

- **fibre-channel npiv-proxy load-balance static**
  - Configures a static mapping between an FCoE port and an FC NP_Port.

- **fibre-channel npiv-proxy load-balance**
  - Configures the NPIV proxy load-balancing method applied to all FC NP_Ports on the switch.

MIB Objects

- **alaFcNpivStaticLoadBalanceTable**
  - **alaFcNpivStaticLoadBalanceFibreIfIndex**
  - **alaFcNpivStaticLoadBalanceEtherIfIndex**
  - **alaFcNpivStaticLoadBalanceRowStatus**

- **alaFcNpivLoadBalSessTable**
  - **alaFcNpivLoadBalSessIfIndex**
  - **alaFcNpivLoadBalSessCount**
clear fibre-channel statistics

Clears FC port statistics.

```
clear fibre-channel statistics [npiv | r-npiv] [port chassis/slot/port[-port2] [e-tunnel port chassis/slot/port[-port2]]
```

### Syntax Definitions

- **npiv**: Clears statistics for N_Prot proxy sessions.
- **r-npiv**: Clears statistics for F_Prot proxy sessions.
- **e-tunnel [tunnel_id]**: Clears E2E tunnel (E_Prot proxy) statistics. Optionally enter a tunnel ID to display information for a specific tunnel.
- **vsan_id [vsan_id2]**: An existing VSAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VSAN IDs (100-150).
- **chassis**: The chassis identifier.
- **slot/port [-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

### Defaults

By default, all statistics are cleared.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `vsan` parameter to clear statistics for a specific VSAN ID. The `vsan` parameter is not used with the `e-tunnel` parameter, because tunnel ports are not associated with a VSAN.

- Use the `port` parameter to clear statistics for a specific FC port.

### Examples

- `clear fibre-channel statistics`
- `clear fibre-channel statistics port 2/2/5`
- `clear fibre-channel statistics npiv`
- `clear fibre-channel statistics r-npiv`
- `clear fibre-channel statistics e-tunnel`
- `clear fibre-channel statistics npiv port 2/2/1`
- `clear fibre-channel statistics r-npiv port 2/2/3`
- `clear fibre-channel statistics e-tunnel port 2/2/4`
**Release History**

Release 7.3.3; command introduced.

**Related Commands**

`show fibre-channel statistics`  Display FC port statistics.

**MIB Objects**

- `alaFcIntfNpivStatsTable`
  - `alaFcIntfNpivStatsIfIndex`
  - `alaFcIntfNpivStatsClear`
- `alaFcVsanNpivStatsTable`
  - `alaFcVsanNpivStatsVsan`
  - `alaFcVsanNpivStatsClear`
- `alaFcIntfRnpivStatsTable`
  - `alaFcIntfRnpivStatsIfIndex`
  - `alaFcIntfRnpivStatsClear`
- `alaFcVsanRnpivStatsTable`
  - `alaFcVsanRnpivStatsVsan`
  - `alaFcVsanRnpivStatsClear`
- `alaFcTidEtunnelStatsTable`
  - `alaFcTidEtunnelStatsTunnelId`
  - `alaFcTidEtunnelStatsClear`
- `alaFcIntfEtunnelStatsTable`
  - `alaFcIntfEtunnelStatsIfIndex`
  - `alaFcIntfEtunnelStatsClear`
clear fibre-channel sessions

Clears the specified sessions on all FC ports.

`clear fibre-channel sessions {npiv-proxy | r-proxy | e-tunnel | all}`

**Syntax Definitions**

- **npiv-proxy**: Clears NP_Port proxy sessions.
- **r-proxy**: Clears reverse NP_Port proxy sessions.
- **e-tunnel**: Clears E-Tunnel (E2E Tunnel) sessions.
- **all**: Clears all NP_Port proxy, reverse proxy, and E-Tunnel sessions.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Only the sessions associated with the specified parameter are cleared. For example, if the `npiv-proxy` parameter is used, only NPIV proxy sessions are cleared. All other session types remain active.
- When sessions are cleared on FC ports, the corresponding sessions on the FCoE ports are also cleared.

**Examples**

- `-> clear fibre-channel sessions npiv-proxy`
- `-> clear fibre-channel sessions r-npiv`
- `-> clear fibre-channel sessions e-tunnel`
- `-> clear fibre-channel sessions all`

**Release History**

Release 7.3.3; command introduced.
Related Commands

show fibre-channel sessions  Displays FC sessions.

MIB Objects

alaFcInfo
   alaFcConfigSessClear
clear fcoe statistics npiv

Clears N_Port proxy (NP_Port) statistics for FCoE interfaces or specific FCoE VLANs.

```
clear fcoe statistics npiv-proxy {interface | vlan [vlan_id|vlan_id2] | port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

### Syntax Definitions

- **interface**: Clears statistics for all FCoE interfaces (ports and link aggregates).
- **vlan_id[vlan_id2]**: An existing FCoE VLAN ID. The valid ID range is 2–4094. Use a hyphen to specify a range of VLAN IDs (100-150).
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- **agg_id[-agg_id2]**: The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

### Defaults

N/A.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8/C32E/T24C2</th>
<th>9900X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `vlan` parameter to clear statistics for a specific FCoE VLAN ID.
- Use the `port` or `linkagg` parameters to clear statistics for a specific FCoE port or link aggregate ID.

### Examples

```
-> clear fcoe statistics npiv-proxy interface
-> clear fcoe statistics npiv-proxy vlan 100
-> clear fcoe statistics npiv-proxy vlan 200-205
-> clear fcoe statistics npiv-proxy port 1/1
-> clear fcoe statistics npiv-proxy port 1/5-10
-> clear fcoe statistics npiv-proxy port 1/1/1
-> clear fcoe statistics npiv-proxy linkagg 10
```
**Release History**

Release 7.3.3; command introduced.

**Related Commands**

`show fcoe statistics npiv-proxy`  Displays N_Port proxy statistics.

**MIB Objects**

- `alaFipsVlanTable`
  - `alaFipsVlanStatsFnreClear`
- `alaFipsIntfTable`
  - `alaFipsIntfStatsFnreClear`
clear fcoe statistics r-npiv

Clears F_Port proxy (reverse-NPIV) statistics for FCoE interfaces or specific FCoE VLANs.

clear fcoe statistics r-npiv {interface | vlan [vlan_id|vlan_id2] | port chassis/slot/port[-port2] | linkagg agg_id[1-agg_id]}]

Syntax Definitions

interface
Clears statistics for all FCoE interfaces (ports and link aggregates).

vlan_id|vlan_id2
An existing FCoE VLAN ID. The valid ID range is 2-4094. Use a hyphen to specify a range of VLAN IDs (100-150).

chassis
The chassis identifier.

slot/port[-port2]
The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

agg_id[1-agg_id]
The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>9900 C32E/T24C2</th>
<th>9900 X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `vlan` parameter to clear statistics for a specific FCoE VLAN ID.
- Use the `port` or `linkagg` parameters to clear statistics for a specific FCoE port or link aggregate ID.

Examples

- `clear fcoe statistics r-npiv interface`
- `clear fcoe statistics r-npiv vlan 100`
- `clear fcoe statistics r-npiv vlan 200-205`
- `clear fcoe statistics r-npiv port 1/1`
- `clear fcoe statistics r-npiv port 1/5-10`
- `clear fcoe statistics r-npiv port 1/1/1`
- `clear fcoe statistics r-npiv linkagg 10`
**Release History**

Release 7.3.3; command introduced.

**Related Commands**

*show fcoe statistics r-npiv*  
Displays F_Port proxy statistics.

**MIB Objects**

alaFipsVlanTable  
   alaFipsVlanStatsFnreClear  
alaFipsIntfTable  
   alaFipsIntfStatsFnreClear
**clear fcoe statistics e-tunnel**

Clears E_Port proxy (E2E tunnel) statistics.

`clear fcoe statistics e-tunnel [ve | te] {tunnel_id|-tunnel_id}`

### Syntax Definitions

- **ve**
  - Clears VE_Port statistics.

- **te**
  - Clears TE_Port statistics.

- **tunnel_id|-tunnel_id**
  - The ID of an existing E2E tunnel. Use a hyphen to specify a range of tunnel IDs (10-15).

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **ve** parameter to clear only VE_Port statistics for the specified tunnel ID.
- Use the **te** parameter to clear only TE_Port statistics for the specified tunnel ID.

### Examples

- `-> clear fcoe statistics e-tunnel 1`
- `-> clear fcoe statistics e-tunnel ve 2`
- `-> clear fcoe statistics e-tunnel te 2`

### Release History

Release 7.3.3; command introduced.
Related Commands

show fcoe statistics e-tunnel  Displays E_Port proxy (E2E tunnel) statistics.

MIB Objects

alaFipsEtunnelVePortStatsTable
  alaFipsEtunnelVePortStatsTunnelId
  alaFipsEtunnelVePortStatsClear
alaFipsEtunnelTePortStatsTable
  alaFipsEtunnelTePortStatsTunnelId
  alaFipsEtunnelTePortStatsClear
clear fcoe sessions

Clears the specified sessions on all FCoE ports.

```
clear fcoe sessions [fips | npiv-proxy | r-proxy | e-tunnel | all]
```

### Syntax Definitions

- **fips**
  - Clears FIP snooping sessions.
- **npiv-proxy**
  - Clears NP_Port proxy sessions.
- **r-proxy**
  - Clears reverse NP_Port proxy sessions.
- **e-tunnel**
  - Clears E-Tunnel (E2E Tunnel) sessions.
- **all**
  - Clears all FCoE, NP_Port proxy, reverse proxy, and E-Tunnel sessions.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When FIP snooping sessions are cleared, a clear virtual link (CVL) request is sent for all logged ENodes.
- When R-NPIV sessions are cleared, FIP FLOGO is sent to the FCF and FC FLOGO is sent to the HBA for each R-NPIV session created.
- Once sessions are cleared, NP_Ports will trigger a fabric login to the connected fabric.

### Examples

- `-> clear fcoe sessions fips`
- `-> clear fcoe sessions npiv-proxy`
- `-> clear fcoe sessions r-proxy`
- `-> clear fcoe sessions e-tunnel`
- `-> clear fcoe sessions all`

### Release History

Release 7.3.3; command introduced.
Related Commands

show fcoe sessions  Displays the FCoE session information for the switch.

MIB Objects

alaFipsInfo
  alaFipsConfigSessClear
45  VXLAN Snooping Commands

The OmniSwitch Virtual eXtensible LAN (VXLAN) Snooping feature attempts to detect and identify VXLAN traffic by sampling packets to determine if they are VXLAN encapsulated packets. Once this type of traffic is identified, VXLAN Snooping collects and stores information about the flow in a database on the local switch. Additional configurable options for this feature include the ability to apply QoS policy list rules to the identified flow and SNMP trap generation.

A VXLAN segment is a Layer 2 overlay network through which devices can communicate. Traffic from such devices is encapsulated into VXLAN frames and then tunneled through the VXLAN segment. Using this implementation of VXLAN Snooping, an administrator can obtain more detailed information about the traffic flow through the overlay network.

**Note.** Throughout this chapter, the terms “VXLAN Snooping” and “VM Snooping” are interchangeable.

MIB information for the VXLAN Snooping commands is as follows:

- **Filename:** ALCATEL-IND1-VM-SNOOPING-MIB.mib
- **Module:** alaVMSnoopingMIB

A summary of the available commands is listed here:

- `vm-snooping admin-state`
- `vm-snooping policy-mode`
- `vm-snooping trap`
- `vm-snooping filtering-resource trap threshold`
- `vm-snooping sampling-rate`
- `vm-snooping aging-timer`
- `vm-snooping vxlan udp-port`
- `vm-snooping static-policy rule`
- `vm-snooping logging-threshold`
- `vm-snooping port`
- `show vm-snooping config`
- `show vm-snooping port`
- `show vm-snooping database`
- `show vm-snooping virtual-machines`
- `show vm-snooping filtering-resource`
- `show vm-snooping statistics`
- `show vm-snooping static-policy`
- `clear vm-snooping database`
- `clear vm-snooping statistics`
vm-snooping admin-state

Configures the global status of the VXLAN Snooping process for the switch.

vm-snooping admin-state {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables VXLAN Snooping for the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables VXLAN Snooping for the switch.</td>
</tr>
</tbody>
</table>

Defaults

By default, VXLAN Snooping is disabled for the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C8/C32E/T24C2/X24C2</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Enable VXLAN Snooping first before attempting any other VXLAN Snooping command. When enabled, the switch allocates resources for this feature. When disabled, switch resources are released for other purposes.
- This command enables or disables this feature on all VXLAN Snooping ports.

Examples

-> vm-snooping admin-state enable
-> vm-snooping admin-state disable

Release History

Release 7.3.4; command was introduced.

Related Commands

show vm-snooping config Displays the VXLAN Snooping configuration for the switch.

MIB Objects

alaVMsnoopingConfig
alaVMSnoopingAdminStatus
**vm-snooping policy-mode**

Configures the allocation of hardware resources for VXLAN Snooping. Use this command to change the policy lookup mode to basic or advanced and specify the number of policies reserved for VXLAN Snooping. In addition, an optional inner header parameter is available to specify if the header of the inner Ethernet frame is tagged or untagged.

```
vm-snooping policy-mode {basic | advance} [policy-resource {extended | default}] [inner-header {tagged | untagged | default}]
```

### Syntax Definitions

- **basic**
  - Reserves resources for VNI, VXLAN UDP port, inner source MAC address, and inner IPv4 source address policy conditions.

- **advance**
  - For IPv4 packets, reserves resources for VNI, VXLAN UDP port, inner source MAC address, inner IPv4 source address, IP protocol, and Layer 4 source and destination port policy conditions.

  - For IPv6 packets, reserves resources for VNI, VXLAN UDP port, inner source IPv6 address, Layer 4 source and destination port for policy conditions.

- **policy-resource extended**
  - Doubles the amount of resources for VXLAN Snooping policies.

- **policy-resource default**
  - Reserves the minimum amount of resources for VXLAN Snooping policies.

- **inner-header tagged**
  - The header of the inner frame is tagged.

- **inner-header untagged**
  - The header of the inner frame is untagged.

- **inner-header default**
  - The header of the inner frame is either tagged or untagged (basic mode) or just tagged (advance mode).

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>[basic</td>
<td>advance]</td>
</tr>
<tr>
<td>[extended</td>
<td>default]</td>
</tr>
</tbody>
</table>

By default, the inner header option is set to the following values based on the current policy lookup mode:

- Basic mode—untagged and tagged header for the inner frame.
- Advanced mode—tagged header for the inner frame.
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

6900 V72/C32
9900

Usage Guidelines

- To change the policy mode, globally disable VXLAN Snooping then make the changes and enable VXLAN Snooping again to apply the changes to the switch. This command is also allowed when the VXLAN Snooping feature is globally disabled.

- When the VXLAN Snooping policy mode is changed, all database and QoS entries are flushed.

- When the VXLAN policy mode is set to `basic`, any QoS policy rules with advanced mode policy conditions will not work. When the mode is set to `advance`, QoS policy rules with basic and advance policy conditions will work.

- When configuring the `inner-header` parameter for `basic` mode, specifying only tagged or only untagged may increase the number of policies allowed. In other words, specifying both tagged and untagged (the default) may reduce the number of policies allowed.

- When configuring the `inner-header` parameter for `advance` mode, specifying both tagged and untagged is not allowed. In this case, the `default` option sets the parameter to tagged.

- Other applications, such as QoS user policies, VLAN Stacking, Application Fingerprinting, DHCP Snooping, Open Flow, IP multicast, and FIP Snooping also use up system resources. Depending on which application comes first, other applications may not be able to get the required hardware resources.

- If the resources are increased by two times (policy-resource extended), then none of the above-mentioned applications can work simultaneously.

- Only one set of hardware resources are reserved for the VXLAN Snooping application when VXLAN Snooping is globally enabled.

Examples

- `-> vm-snooping admin-state disable`
- `-> vm-snooping policy-mode basic policy-resource extended inner-header tagged`
- `-> vm-snooping admin-state enable`

- `-> vm-snooping admin-state disable`
- `-> vm-snooping policy-mode advance policy-resource extended inner-header untagged`
- `-> vm-snooping admin-state enable`

- `-> vm-snooping admin-state disable`
- `-> vm-snooping policy-mode basic inner-header default`
- `-> vm-snooping policy-mode advance inner-header default`
- `-> vm-snooping admin-state enable`
**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

`show vm-snooping config`  Displays the VXLAN Snooping configuration for the switch.

**MIB Objects**

alaVMSnoopingConfig
   alaVMSnoopingPolicyMode
   alaVMSnoopingPolicyResource
   alaVMSnoopingVMTrafficTagged
**vm-snooping trap**

Enables or disables trap generation for the VXLAN Snooping feature.

```bash
vm-snooping trap {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables VXLAN Snooping trap generation.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables VXLAN Snooping trap generation.</td>
</tr>
</tbody>
</table>

### Defaults

By default, trap generation for this feature is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

A trap is generated when one of the following occurs:

- A new VXLAN database entry is learned or ages out.
- The usage of system resources allocated for VXLAN Snooping exceeds a configurable threshold value.

### Examples

```bash
-> vm-snooping trap enable
-> vm-snooping trap disable
```

### Release History

Release 7.3.4; command was introduced.
**Related Commands**

**vm-snooping filtering-resource trap threshold**
Configures the threshold value at which point the switch generates a trap to indicate that VXLAN Snooping has utilized the specified level of system resources.

**show vm-snooping config**
Displays the VXLAN Snooping status and configuration for the switch.

**MIB Objects**

alaVMSnoopingConfig
alaVMSnoopingTrapStatus
vm-snooping filtering-resource trap threshold

Configures the threshold value at which point the switch generates a trap to indicate that VXLAN Snooping has utilized the specified level of system resources.

```
vm-snooping filtering-resource trap threshold {percentage | default}
```

### Syntax Definitions
- **percentage**: The percentage of system resources used by VXLAN Snooping.
- **default**: Sets the trap threshold value back to 80 percent (the default).

### Defaults
By default, the filtering resource threshold is set to 80 percent.

### Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines
A trap is generated when the system resources used by VXLAN Snooping reach the specified threshold value.

### Examples
- `-> vm-snooping filtering-resource trap threshold 50`
- `-> vm-snooping filtering-resource trap threshold default`

### Release History
Release 7.3.4; command was introduced.
Related Commands

- **show vm-snooping config**
  Displays the VXLAN Snooping status and configuration for the switch.

- **show vm-snooping filtering-resource**
  Displays the system resources used by VXLAN Snooping on a per-port basis.

MIB Objects

- `alaVMSnoopingConfig`
- `alaVMSnoopingFilteringResourceTrapThreshold`
**vm-snooping sampling-rate**

Configures the packets-per-second (pps) sampling rate for the VXLAN Snooping feature.

`vm-snooping sampling-rate pps`

---

**Syntax Definitions**

`pps` The number of packets-per-second to sample on all VXLAN Snooping ports. The valid range is 1–1000.

---

**Defaults**

By default, the sampling rate is set to 1000 pps.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The sampling rate value specified with this command is applied to every VXLAN Snooping port on the switch.

---

**Examples**

- `vm-snooping sampling-rate 500`
- `vm-snooping sampling-rate 1000`

---

**Release History**

Release 7.3.4; command was introduced.

---

**Related Commands**

- **show vm-snooping config** Displays the VXLAN Snooping status and configuration for the switch.

---

**MIB Objects**

- `alaVMSnoopingConfig`  
- `alaVMSnoopingSamplingRate`
vm-snooping aging-timer

Configures the aging time value for VXLAN packet flows learned in the VXLAN Snooping database on the local switch.

```
vm-snooping aging-timer seconds
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>seconds</th>
<th>The number of seconds to wait before aging out a learned VM. The valid range is 60–86400 seconds.</th>
</tr>
</thead>
</table>

**Defaults**

By default, the aging timer is set to 300 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Set this timer to zero to prevent the learned VMs from aging out.
- Note that an inactive VXLAN packet flow (no packets received for the flow) can take up to twice as long as the aging time value specified to be removed from the VXLAN Snooping database. For example, if an aging time of 300 seconds is specified, the database entry for the flow ages out any time between 300 and 600 seconds of inactivity.

**Examples**

```
-> vm-snooping aging-timer 100
-> vm-snooping aging-timer 300
-> vm-snooping aging-timer 0
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

**show vm-snooping config**  
Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

alaVMSnoopingConfig
alaVMSnoopingAgingTimer
**vm-snooping vxlan udp-port**

Configures additional UDP destination port numbers to look for when the switch inspects packets received on VXLAN Snooping ports. This value is used to identify encapsulated VXLAN packets.

```bash
vm-snooping vxlan udp-port {udp_port_num[-udp_port_num2]}
no vm-snooping vxlan udp-port {udp_port_num[-udp_port_num2]}
```

**Syntax Definitions**

`udp_port_num[-udp_port_num2]` The UDP destination port number. Use a hyphen to specify a range of port numbers. Do not specify a range that configures more than seven UDP ports.

**Defaults**

By default, the well-known UDP port number 4789 is used.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release History</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a UDP destination port number. Note that the default UDP port number of 4789 is not configurable, so it can not be removed with this command. Only port numbers that were added through this command can be removed.
- Avoid using the well-known UDP ports that are already reserved by IANA for other applications.
- Including the default UDP port number (4789), up to eight UDP ports are allowed. However, configuring multiple UDP ports may slow down the VXLAN Snooping process.
- Changing the UDP port number on the fly might stop the VXLAN traffic until the VXLAN Tunnel End Points (VTEPs) in the network are configured with the same destination UDP port.

**Examples**

```
-> vm-snooping vxlan udp-port 8472
-> no vm-snooping vxlan udp-port 8472
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

**show vm-snooping config**  Displays the destination UDP port value that is used to identify VXLAN traffic.

MIB Objects

alaVMSnoopingUDPPortTable
- alaVMSnoopingUDPPortIndex
- alaVMSnoopingUDPRowStatus
vm-snooping static-policy rule

Configures a static QoS policy rule. When configured, QoS resources are automatically allocated for the specified rule even if there is no VXLAN packet flow that matches the rule conditions.

**Syntax**

```plaintext
vm-snooping static-policy rule rule_name [list list_name]
no vm-snooping static-policy rule rule_name [list list_name]
```

**Syntax Definitions**

- **rule_name**: The name of the policy rule (alphanumeric string up to 32 characters).
- **list_name**: The name of the policy list (alphanumeric string up to 32 characters).

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_name</td>
<td>“Default”</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a static VXLAN Snooping policy rule. If the rule is associated with a user-configured policy list (not the default list), then the list name must be specified as well to remove the static policy rule. If the rule is associated with the default list, then specifying a list name is not required to remove the static policy rule.

- The default policy list available in every switch has no name and is not configurable. All QoS policy rules are assigned to the default list unless the **no default-list** option of the **policy rule** command is used at the time the rule is created.

**Examples**

- `vm-snooping static-policy rule r1`
- `vm-snooping static-policy rule r2 list 12`
- `no vm-snooping static-policy rule r1`
- `no vm-snooping static-policy rule r2 list 12`

**Release History**

Release 7.3.4; command was introduced.
Related Commands

*show vm-snooping static-policy*  Displays the static policy configuration.

**MIB Objects**

alaVMSnoopingStaticPolicyTable

alaVMSnoopingStaticPolicyRuleName

alaVMSnoopingStaticPolicyListName

alaVMSnoopingStaticPolicyRowStatus
vm-snooping logging-threshold

Configures the threshold value that determines how many entries for VXLAN packet flows and statistics are logged into a .csv file on the local switch.

```
vm-snooping logging-threshold number-of-flows \{flow_num | default\}
```

**Syntax Definitions**

- `flow_num`: The number of VXLAN packet flows to log. The range is 1000–6000.
- `default`: Sets the logging threshold value back to 5000 (the default).

**Defaults**

By default, the logging threshold value is set to 5000 packet flows.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Set the logging threshold value to zero to turn off the logging function.
- When the logging function is on, setting the VXLAN Snooping aging timer to 300 seconds is recommended. If the aging timer is set to zero, no logging occurs regardless of this threshold setting.
- The packet flows and hardware statistics are logged to the `vm_snoop_db_flow_rec.csv` file and the `vm_snoop_hw_stats_rec.csv` file in the `/flash/switch/bridge/vm_snoop/` directory on the local switch to maintain a packet flow history.
- When the number of records logged to the .csv files exceeds the logging threshold value, the corresponding files are renamed to `/flash/switch/bridge/vm_snoop/vm_snoop_db_flow_old_rec.csv` and `/flash/switch/bridge/vm_snoop_hw_stats_old_rec.csv`.
- These files are accessed and used by Alcatel-Lucent Enterprise network management tools to provide management and visibility of the overlay network traffic.

**Examples**

```
-> vm-snooping logging-threshold number-of-flows 1000
-> vm-snooping logging-threshold number-of-flows 0
-> vm-snooping logging-threshold number-of-flows default
```
**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

`show vm-snooping config` Displays the VXLAN Snooping status and configuration for the switch.

**MIB Objects**

alaVMSnoopingConfig

alaVMSnoopingLoggingThresholdFlows
vm-snooping port

Configures a switch port or link aggregate as a VXLAN Snooping interface. Once the interface is configured and enabled and VXLAN Snooping is enabled for the switch, IP packets received on the interface are sampled to determine if they contain the designated UDP destination port.

```
vm-snooping {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [admin-state {enable | disable}]
```

```
no vm-snooping {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
```

### Syntax Definitions

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).
- `enable` Enables the VXLAN Snooping administrative status on the port or link aggregate ID.
- `disable` Disables the VXLAN Snooping administrative status on the port or link aggregate ID.

### Defaults

By default, VXLAN Snooping is disabled on all switch ports and link aggregates.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to revert the VXLAN Snooping interface back to a regular switch port or link aggregate. This will clear the VXLAN Snooping configuration from the interface.
- Disabling the administrative status of a VXLAN Snooping interface does not remove the VXLAN Snooping configuration from the interface.
- Make sure the VXLAN Snooping feature is globally enabled for the switch to ensure that VXLAN Snooping ports will process VXLAN packets.
- VXLAN Snooping uses the sFlow mechanism to sample packets.
Examples
-> vm-snooping port 1/1/1
-> vm-snooping port 1/1/5-10
-> no vm-snooping port 1/1/1
-> no vm-snooping port 1/1/5-10
-> vm-snooping port 1/1/1 admin-state enable
-> vm-snooping port 1/1/5-10 admin-state enable
-> vm-snooping port 1/1/1 admin-state disable
-> vm-snooping port 1/1/5-10 admin-state disable

-> vm-snooping linkagg 1
-> vm-snooping linkagg 5-10
-> no vm-snooping linkagg 1
-> no vm-snooping linkagg 5-10
-> vm-snooping linkagg 1 admin-state enable
-> vm-snooping linkagg 5-10 admin-state enable
-> vm-snooping linkagg 1 admin-state disable
-> vm-snooping linkagg 5-10 admin-state disable

Release History
Release 7.3.4; command was introduced.

Related Commands
vm-snooping admin-state  Configures the global VXLAN Snooping status for the switch.
show vm-snooping port  Displays the VXLAN Snooping port configuration.

MIB Objects
alaVMSnoopingPortTable
  alaVMSnoopingPortIndex
  alaVMSnoopingPortAdminStatus
  alaVMSnoopingPortIsVNP
  alaVMSnoopingPortRowStatus
show vm-snooping config

Displays the global VXLAN Snooping status and configuration information for the switch.

show vm-snooping config

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples

-> show vm-snooping config
VM-Snooping Status : Enable,
Trap : Disable,
Trap-Threshold : 80,
Policy-Mode : Basic
Policy-Resource : Default
VM Inner Header : Tagged and Untagged,
Aging-Timer : 300 seconds,
UDP-Port(s) : 4789,
Sampling-Rate : 1000
Logging-Threshold : 5000
Qos Allocation Status : Success

output definitions

VM-Snooping Status The global administrative status of VXLAN Snooping for the switch (Enabled or Disabled). Configured through the vm-snooping admin-state command.

Trap The status of SNMP trap generation for the switch (Enabled or Disabled). Configured through the vm-snooping trap command.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trap-Threshold</td>
<td>The percentage of switch resources used that will trigger the switch to generate a trap. Configured through the <code>vm-snooping filtering-resource trap threshold</code> command.</td>
</tr>
<tr>
<td>Policy-Mode</td>
<td>The policy mode setting that designates switch resources for VXLAN Snooping. Configured through the <code>vm-snooping policy-mode</code> command.</td>
</tr>
<tr>
<td>Policy Resource</td>
<td>Indicates the number of VXLAN Snooping policies allowed (Default or Extended). Configured through the <code>vm-snooping policy-mode</code> command.</td>
</tr>
<tr>
<td>VM Inner Header</td>
<td>Whether to check tagged and/or untagged VM traffic. Configured through the <code>vm-snooping policy-mode</code> command.</td>
</tr>
<tr>
<td>Aging-Timer</td>
<td>The number of seconds before a learned VM is aged out. Configured through the <code>vm-snooping aging-timer</code> command.</td>
</tr>
<tr>
<td>UDP-Port(s)</td>
<td>The UDP port numbers to snoop for VXLAN packets. Configured through the <code>vm-snooping vxlan udp-port</code> command.</td>
</tr>
<tr>
<td>Sampling-Rate</td>
<td>The number of packets-per-second (pps) to sample. Configured through the <code>vm-snooping sampling-rate</code> command.</td>
</tr>
<tr>
<td>Logging-Threshold</td>
<td>The number of VXLAN packet flow entries and statistics logged to a <code>.csv</code> file on the local switch.</td>
</tr>
<tr>
<td>Qos Allocation Status</td>
<td>The status of QoS resource allocation (Success, inProgress, or Failed). This field is blank when VXLAN Snooping is disabled.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `show vm-snooping port` Displays the VXLAN Snooping port configuration.

**MIB Objects**

- `alaVMSnoopingConfig`
- `alaVMSnoopingAdminStatus`
- `alaVMSnoopingPolicyMode`
- `alaVMSnoopingPolicyResource`
- `alaVMSnoopingVMTrafficTagged`
- `alaVMSnoopingTrapStatus`
- `alaVMSnoopingFilteringResourceTrapThreshold`
- `alaVMSnoopingAgingTimer`
- `alaVMSnoopingSamplingRate`
- `alaVMSnoopingLoggingThresholdFlows`
- `alaVMSnoopingQosAllocationStatus`
- `alaVMSnoopingUdpPortTable`
- `alaVMSnoopingUdpPortIndex`
- `alaVMSnoopingUdpRowStatus`
show vm-snooping port

Displays the VXLAN Snooping port configuration for the switch.

show vm-snooping port

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the port and linkagg parameters to display information for a specific port or link aggregate.
- The display output also indicates whether or not the VXLAN Snooping port is a virtual machine network profile (vNP) port.

Examples

```shell
-> show vm-snooping port
Port VM-Snooping vNP
-------+------------+--------
1/2/1  Enable        Yes
1/2/2  Enable        No
1/2/2  Enable        Yes
1/2/2  Enable        Yes
0/12   Disable       No
```

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The slot/port or link aggregate ID of the VXLAN Snooping interface. A</td>
</tr>
<tr>
<td></td>
<td>&quot;0&quot; slot number indicates that the interface is a link aggregate.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VM-Snooping</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The administrative status (Enable or Disable) of VXLAN Snooping on the port</td>
</tr>
<tr>
<td></td>
<td>or link aggregate. Configured through the vm-snooping port command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>vNP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Whether the port is also a vNP port (Yes or No).</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

- `show vm-snooping config` Displays the VXLAN Snooping status and configuration for the switch.

**MIB Objects**

- `alaVMSnoopingPortTable`
  - `alaVMSnoopingPortIndex`
  - `alaVMSnoopingPortAdminStatus`
  - `alaVMSnoopingPortIsVNP`
  - `alaVMSnoopingPortRowStatus`
show vm-snooping database

Displays VXLAN Snooping database entries. When a VXLAN packet is detected and the packet contains the designated UDP destination port, VXLAN Snooping creates an entry in the local switch database to identify and track the VXLAN packet flow.

```
show vm-snooping database [vxlan udp-port udp_port_num | vtep-ip ip_address | vni vxlan_id | vm-src-mac mac_address | vm-ip ip_address] [detail] [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] [detail]
```

**Syntax Definitions**

- `udp_port_num` The UDP destination port number used to identify VXLAN traffic.
- `vtep-ip ip_address` The IP address of the VXLAN Tunnel End Point (VTEP). This is the Loopback0 interface address on the OmniSwitch.
- `vxlan_id` The VXLAN Network Identifier (VNI) for the VXLAN segment on which the VM was learned.
- `mac_address` The source MAC address of a VM.
- `vm-ip ip_address` The source IP address of a VM.
- `detail` Displays additional information about the classified traffic flow.
- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

By default, all database entries are displayed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>C32E/T24C2</td>
<td>X24C2</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `port` and `linkagg` parameters to display information for a specific port or link aggregate.
- Each database entry is subject to a VXLAN Snooping aging period. If the database fills up, older entries are aged out before the limit (fast aging).
- When a database entry is removed due to regular aging or fast aging conditions, any corresponding QoS is also removed for that flow.
Examples

-> show vm-snooping database
Total number of VM Flows: 15

<table>
<thead>
<tr>
<th>VXLAN Port</th>
<th>VNI</th>
<th>VM SRC MAC</th>
<th>VLAN</th>
<th>SRC IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:12:01:00:00:01</td>
<td>-</td>
<td>200.200.200.1</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:12:01:00:00:02</td>
<td>-</td>
<td>200.200.200.2</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:12:01:00:00:03</td>
<td>-</td>
<td>200.200.200.3</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:12:01:00:00:04</td>
<td>-</td>
<td>200.200.200.4</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:12:01:00:00:05</td>
<td>-</td>
<td>200.200.200.5</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:00</td>
<td>-</td>
<td>2.0.0.0</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:01</td>
<td>-</td>
<td>2.0.0.1</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:02</td>
<td>-</td>
<td>2.0.0.2</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:03</td>
<td>-</td>
<td>2.0.0.3</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:04</td>
<td>-</td>
<td>2.0.0.4</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:01</td>
<td>8</td>
<td>88.0.0.1</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:02</td>
<td>8</td>
<td>88.0.0.2</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:03</td>
<td>8</td>
<td>88.0.0.3</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:04</td>
<td>8</td>
<td>88.0.0.4</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:05</td>
<td>8</td>
<td>88.0.0.5</td>
</tr>
</tbody>
</table>

-> show vm-snooping database port 1/2/2
Total number of VM Flows: 5

<table>
<thead>
<tr>
<th>VXLAN Port</th>
<th>VNI</th>
<th>VM SRC MAC</th>
<th>VLAN</th>
<th>SRC IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:01</td>
<td>8</td>
<td>88.0.0.1</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:02</td>
<td>8</td>
<td>88.0.0.2</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:03</td>
<td>8</td>
<td>88.0.0.3</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:04</td>
<td>8</td>
<td>88.0.0.4</td>
</tr>
<tr>
<td>1/2/2</td>
<td>4789</td>
<td>00:00:00:88:00:05</td>
<td>8</td>
<td>88.0.0.5</td>
</tr>
</tbody>
</table>

-> show vm-snooping database vni 1234
Total number of VM Flows: 5

<table>
<thead>
<tr>
<th>VXLAN Port</th>
<th>VNI</th>
<th>VM SRC MAC</th>
<th>VLAN</th>
<th>SRC IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:00</td>
<td>-</td>
<td>2.0.0.0</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:01</td>
<td>-</td>
<td>2.0.0.1</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:02</td>
<td>-</td>
<td>2.0.0.2</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:03</td>
<td>-</td>
<td>2.0.0.3</td>
</tr>
<tr>
<td>1/1/3</td>
<td>4789</td>
<td>00:00:04:00:00:04</td>
<td>-</td>
<td>2.0.0.4</td>
</tr>
</tbody>
</table>

output definitions

Port       The slot/port or link aggregate ID of the VXLAN Snooping interface. A “0” slot number indicates a link aggregate.
VXLAN Port  The UDP port for the VXLAN segment.
VNI         The VXLAN Network ID (VNI) for the VXLAN segment on which the VM was learned.
VM SRC MAC  The source MAC address of the VM.
-> show vm-snooping database detail
Total number of VM Flows: 2

| Port:                        | 1/1/3,                 |
| VTEP SRC IP:                | 100.0.1.1,             |
| VTEP DEST IP:               | 100.0.1.2,             |
| VTEP VLAN:                  | 100,                   |
| VXLAN VNI:                  | 2000,                  |
| VXLAN PORT:                 | 4789,                  |
| VM SRC MAC:                 | 00:12:01:00:00:01:01,  |
| VM DEST MAC:                | 00:14:01:00:00:01:01,  |
| VM VLAN:                    | UnTagged,              |
| VM SRC IP/PORT:             | 200.200.200.1/1,       |
| VM DEST IP/PORT:            | 200.200.200.2/515,     |
| VM IP PROTO:                | 61,                    |
| POLICY RULE:                | r1,                    |
| POLICY LIST:                | Default,               |
| SAMPLED PKTS                | 170,                   |
| LEARNED TIME                | Mon Dec 15 11:58:50 2014 |

| Port:                        | 1/1/3,                 |
| VTEP SRC IP:                | 100.0.2.1,             |
| VTEP DEST IP:               | 100.0.2.2,             |
| VTEP VLAN:                  | 100,                   |
| VXLAN VNI:                  | 2001,                  |
| VXLAN PORT:                 | 4789,                  |
| VM SRC MAC:                 | 00:12:01:00:00:02:01,  |
| VM DEST MAC:                | 00:14:01:00:00:02:01,  |
| VM VLAN:                    | UnTagged,              |
| VM SRC IP/PORT:             | 200.200.201.1/1,       |
| VM DEST IP/PORT:            | 200.200.201.2/515,     |
| VM IP PROTO:                | 61,                    |
| POLICY RULE:                | r2,                    |
| POLICY LIST:                | Default,               |
| SAMPLED PKTS                | 177,                   |
| LEARNED TIME                | Mon Dec 15 11:58:50 2014 |

**output definitions (continued)**

| VM VLAN | The VLAN ID tag for the VM packet. |
| VM SRC IP | The source IP address of the VM. |

**Port**

The slot/port or link aggregate ID of the VXLAN Snooping interface. A “0” slot number indicates a link aggregate.

**VTEP SRC IP**

The source IP network address for the VTEP.

**VTEP DST IP**

The destination IP network address for the VTEP.

**VTEP VLAN**

The VLAN ID associated with the VTEP.

**VXLAN VNI**

The VNI for the VXLAN segment on which the VM was learned.

**VXLAN Port**

The UDP port for the VXLAN segment.

**VM SRC MAC**

The source MAC address for the VM.

**VM DEST MAC**

The destination MAC address for the VM.

**VM VLAN**

The VLAN on which the VM is learned and forwarded.
### VXLAN Snooping Commands

#### show vm-snooping database

<table>
<thead>
<tr>
<th>VM SRC IP/PORT</th>
<th>The source IP address of the VM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM DEST IP/PORT</td>
<td>The destination IP address of the VM.</td>
</tr>
<tr>
<td>VM IP PROTO</td>
<td>The IP protocol version for the VM.</td>
</tr>
<tr>
<td>POLICY RULE</td>
<td>The name of the QoS policy rule applied to the VM flow.</td>
</tr>
<tr>
<td>POLICY LIST</td>
<td>The name of the QoS policy list applied to the VM flow.</td>
</tr>
<tr>
<td>SAMPLED PKTS</td>
<td>The number of packets sampled for this flow.</td>
</tr>
<tr>
<td>LEARNED TIME</td>
<td>The date and time the flow entry was learned.</td>
</tr>
</tbody>
</table>

#### Release History

Release 7.3.4; command was introduced.

#### Related Commands

- **clear vm-snooping database**: Clears the local database entries for each virtual machine (VM) flow.
- **show vm-snooping config**: Displays the VXLAN Snooping configuration for the switch.
- **show vm-snooping port**: Displays the VXLAN Snooping port configuration.

#### MIB Objects

- `alaVMSnoopingDBTable`  
- `alaVMSnoopingDBFlowId`  
- `alaVMSnoopingDBIfIndex`  
- `alaVMSnoopingDBVxlanUdpDestPort`  
- `alaVMSnoopingDBVni`  
- `alaVMSnoopingDBVtepVlan`  
- `alaVMSnoopingDBVtepSrcIpAddrType`  
- `alaVMSnoopingDBVtepSrcIpAddr`  
- `alaVMSnoopingDBVtepDestIpAddrType`  
- `alaVMSnoopingDBVtepDestIpAddr`  
- `alaVMSnoopingDBInnerSrcMacAddr`  
- `alaVMSnoopingDBInnerDestMacAddr`  
- `alaVMSnoopingDBInnerVlan`  
- `alaVMSnoopingDBInnerSrcIpAddrType`  
- `alaVMSnoopingDBInnerSrcIpAddr`  
- `alaVMSnoopingDBInnerDestIpAddrType`  
- `alaVMSnoopingDBInnerDestIpAddr`  
- `alaVMSnoopingDBVInnerL4SrcPort`  
- `alaVMSnoopingDBVInnerL4DestPort`  
- `alaVMSnoopingDBVInnerIPProtocol`  
- `alaVMSnoopingDBPolicyRule`  
- `alaVMSnoopingDBPolicyList`  
- `alaVMSnoopingDBSamplingStatsPackets`
clear vm-snooping database

Clears the local database entries for each virtual machine (VM) flow.

`clear vm-snooping database [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]`

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]` The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

By default, all database entries are cleared for all VXLAN Snooping ports and link aggregates.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No/Yes/No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `port` and `linkagg` parameters to clear database entries for a specific port or link aggregate.

**Examples**

- `-> clear vm-snooping database`
- `-> clear vm-snooping database port 3/1/1`
- `-> clear vm-snooping database linkagg 10`

**Release History**

Release 7.3.4; command introduced.
Related Commands

**show vm-snooping database**  Displays the contents of the VXLAN Snooping database.

MIB Objects

alaVMSnoopingConfig
- alaVMSnoopingClearAllData
alaVMSnoopingDBTable
- alaVMSnoopingDBClearStats
show vm-snooping virtual-machines

Displays the port, source MAC address, and VLAN associated with Virtual Machines (VMs) discovered through the VXLAN Snooping process.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

The output display of this command shows the port, source MAC address, and VLAN associated with each VM learned through the VXLAN Snooping process.

Examples

```
-> show vm-snooping virtual-machines
Port SRC MAC VLAN
-------- ----------------- +-----+
1/1/2 00:00:00:88:00:01 -
1/1/2 00:00:00:88:00:02 -
1/1/2 00:00:00:88:00:03 -
1/1/2 00:00:00:88:00:04 -
1/1/2 00:00:00:88:00:05 -
```

output definitions

Port: The slot/port or link aggregate ID of the VXLAN Snooping interface. A “0” slot number indicates a link aggregate.

SRC MAC: The source MAC address of the VM.

VLAN: The VLAN on which the VM is learned and forwarded.

Release History

Release 7.3.4; command was introduced.
Related Commands

show vm-snooping config  Displays the VXLAN Snooping configuration for the switch.
show vm-snooping database Displays the contents of the local VXLAN Snooping database.

MIB Objects

alaVMSnoopingLearntVMTable
  alaVMSnoopingLearntVMIIfIndex,
  alaVMSnoopingLearntVMSrcMac,
  alaVMSnoopingLearntVMVlanId
**show vm-snooping filtering-resource**

Displays the amount of switch resources available for and used by QoS policies that contain VXLAN conditions.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- VXLAN Snooping uses the amount of resources used to calculate the percentage of switch resources used and then determine if that percentage exceeds the value set for the filtering trap threshold. An SNMP trap is generated when the percentage used meets or exceeds the trap threshold value.
- The output display of this command shows the percentage of switch resources used by VXLAN policies on a per-slot basis.

**Examples**

```bash
-> show vm-snooping filtering-resource
Total Filtering Resources :256,
Chassis/Slot Filtering Resources Used
-------------------------+-------------------------------
 1/SLOT-1                0
 2/SLOT-1                0
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

**vm-snooping filtering-resource**  
Configures the trap threshold value for system resources used by VXLAN Snooping.

**trap threshold**  

**show vm-snooping config**  
Displays the VXLAN Snooping status and configuration for the switch.

MIB Objects

alaVMSnoopingFilterResourceTable
  - alaVMSnoopingFilterResourceChassisId
  - alaVMSnoopingFilterResourceSlotNum
  - alaVMSnoopingFilterResourceMax
  - alaVMSnoopingFilterResourceUsed
**show vm-snooping statistics**

Displays statistics for each VXLAN packet flow on a VXLAN Snooping port or link aggregate.

```
show vm-snooping statistics [hardware | sampling] [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]
```

---

**Syntax Definitions**

**hardware**
Displays the VXLAN policy rule and list and the number of packets and bytes on which the policy rule was applied.

**sampling**
Displays the number of VXLAN packets that were sampled for a specific flow.

**chassis**
The chassis identifier.

**slot/port[-port2]**
The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

**agg_id[-agg_id2]**
The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

---

**Defaults**

By default, statistics are displayed for all VXLAN Snooping ports and link aggregates.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the **port** and **linkagg** parameters to display information for a specific port or link aggregate.

---

**Examples**

```
-> show vm-snooping statistics
Total number of Hardware Statistics: 0

Policy Rule                     Policy List       Number of pkts       Number of Bytes
---------------------------------+------------------+---------------------+------------------+
Total number of Sampling Statistics: 1

                  VXLAN   VXLAN     VM   VM   Pkts
Port  UDP PORT  VNI  SRC_MAC  SRC_IP
---------------------------------+------------------+---------------------+------------------+
2/1/2   4789     43 00:00:00:88:00:01  88.0.0.1  15
```

---

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023
-> show vm-snooping statistics sampling
Total number of Sampling Statistics: 1

<table>
<thead>
<tr>
<th>Port</th>
<th>VXLAN</th>
<th>VNI</th>
<th>VM</th>
<th>VM</th>
<th>Pkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>4789</td>
<td>43</td>
<td>00:00:00:99:00:01</td>
<td>99.0.0.1</td>
<td>10</td>
</tr>
</tbody>
</table>

-> show vm-snooping statistics hardware
Total number of Hardware Statistics: 1

<table>
<thead>
<tr>
<th>Policy Rule</th>
<th>Policy List</th>
<th>Number of pkts</th>
<th>Number of Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>r1</td>
<td>Default</td>
<td>497</td>
<td>45724</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.4; command introduced.

**Related Commands**

`clear vm-snooping statistics`  Clears VXLAN Snooping statistics.

**MIB Objects**

alaVMSnoopingHardwareStatsTable
- alaVMSnoopingHardwareStatsPolicylist
- alaVMSnoopingHardwareStatsPolicyrule
- alaVMSnoopingHardwareStatsNumOfPackets
- alaVMSnoopingHardwareStatsNumOfBytes
**show vm-snooping static-policy**

Displays the static QoS policy rule configuration for VXLAN Snooping.

Show vm-snooping static-policy

---

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When a static policy rule is configured for VXLAN Snooping, QoS resources are automatically allocated for the specified rule even if there is no VXLAN packet flow that matches the rule conditions.

- If the static policy rule was created with a user-configured policy list (not the default list), then the list name appears in the “Policy List” field. However, if the static policy rule was created without specifying a policy list name, then the “Default” list name appears in the “Policy List” field.

### Examples

```plaintext
-> show vm-snooping static-policy
Total number of Static-Policy: 5

Policy Rule    | Policy List
---------------|----------------
r0             | Default
r1             | Default
r2             | L1
r2             | L3
r2             | Default
```

### Output Definitions

- **Policy Rule**: The name of the QoS policy rule that was specified when the static policy rule was created.
- **Policy List**: The name of the QoS policy list associated with the static policy rule.
**Release History**

Release 7.3.4; command was introduced.

**Related Commands**

*vm-snooping static-policy rule*  Configures a VXLAN Snooping static policy rule.

**MIB Objects**

alaVMSnoopingStaticPolicyTable
  alaVMSnoopingStaticPolicyRuleName
  alaVMSnoopingStaticPolicyListName
  alaVMSnoopingStaticPolicyRowStatus
clear vm-snooping statistics

Clears the collected statistics for each VXLAN packet flow on a VXLAN Snooping port or link aggregate.

```
clear vm-snooping statistics [sampling [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]] [hardware]
```

**Syntax Definitions**

- `chassis`  The chassis identifier.
- `slot/port[-port2]`  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `agg_id[-agg_id2]`  The link aggregate ID number. Use a hyphen to specify a range of IDs (10-20).

**Defaults**

By default, statistics are cleared on all VXLAN Snooping ports and link aggregates.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `port` and `linkagg` parameters to clear statistics for a specific port or link aggregate.

**Examples**

- `clear vm-snooping statistics`
- `clear vm-snooping statistics sampling port 3/1/1`
- `clear vm-snooping statistics sampling linkagg 10`
- `clear vm-snooping statistics hardware`

**Release History**

Release 7.3.4; command introduced.
Related Commands

show vm-snooping statistics  Displays VXLAN Snooping statistics.

MIB Objects

alaVMSnoopingConfig
  alaVMSnoopingClearAllData
alaVMSnoopingSamplingStatsTable
  alaVMSnoopingSamplingStatsClear
Port Mapping is a security feature that controls communication between peer users. Each session comprises of a session ID and a set of user ports and/or a set of network ports. The user ports within a session cannot communicate with each other and can only communicate through network ports. In a port mapping session with user port set A and network port set B, ports in set A can communicate with ports in set B only. If set B is empty, the ports in set A can communicate with the rest of the ports in the system.

A port mapping session can be configured in a unidirectional or bidirectional mode. In the unidirectional mode, the network ports can communicate with each other within the same session. In the bidirectional mode, the network ports cannot communicate with each other. Network ports of a unidirectional port mapping session can be shared with other unidirectional sessions, but cannot be shared with any session that is configured in bidirectional mode. Network ports of different sessions can communicate with each other.

MIB information for the Port Mapping commands is as follows:

- **Filename**: ALCATEL-IND1-PORT-MAPPING.mib
- **Module**: alcatelIND1PortMappingMIB

A summary of the available commands is listed here:

```
port-mapping user-port network-port
port-mapping (configures port mapping status and direction)
port-mapping unidirectional bidirectional
port-mapping unknown-unicast-flooding
port-mapping dynamic-proxy-arp
show port-mapping status
show port-mapping
show ip dynamic-proxy-arp
```
**port-mapping user-port network-port**

Creates a port mapping session with the user ports, network ports, or both user ports and network ports. Use the **no** form of the command to delete ports or a link aggregate group from a session.

```
port-mapping session_id [user-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id}] [network-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id}]
no port-mapping session_id [user-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id}] [network-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id}]
```

### Syntax Definitions

- **session_id**
  - The port mapping session ID.
- **user-port**
  - Specifies a user port of the mapping session.
- **network-port**
  - Specifies a network port of the mapping session.
- **chassis**
  - The chassis identifier.
- **slot**
  - The slot number to be assigned to the mapping session.
- **slot/port[-port2]**
  - The slot and port number to assign to the mapping session. Use a hyphen to specify a range of ports (1/5-10).
- **agg_id**
  - The link aggregate ID number to assign to the mapping session.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- User ports that are part of one session cannot communicate with each other. The user ports can communicate only through network ports of the session to the other elements of the system.
- User ports can be part of only one port mapping session.
- An aggregable port of a link aggregation group cannot be a mapped port and a mapped port cannot be an aggregable port of a link aggregation group.
- A mirrored port cannot be a mapped port and a mapped port cannot be a mirrored port.
**Examples**

- `port-mapping 3 user-port 2/3 network-port 6/4`
- `port-mapping 4 user-port 2/5-8`
- `port-mapping 5 user-port 2/3 network-port slot 3`
- `no port-mapping 5 user-port 2/3`
- `no port-mapping 6 network-port linkagg 7`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `port-mapping` Enables, disables, or deletes a port mapping session.
- `port-mapping unidirectional` Configures the direction of a port mapping session.
- `port-mapping bidirectional` Enables or disables flooding of unknown unicast traffic from all ports to user ports for a particular session.
- `port-mapping unknown-unicast-flooding` Displays the configuration of one or more port mapping sessions.
- `show port-mapping` MIB Objects

<table>
<thead>
<tr>
<th>PortMappingSessionTable</th>
<th>pmapSessionNumber</th>
</tr>
</thead>
<tbody>
<tr>
<td>portMappingTable</td>
<td>pmapPortIfindex</td>
</tr>
<tr>
<td></td>
<td>pmapPortType</td>
</tr>
</tbody>
</table>
**port-mapping**

Enables, disables, or deletes a port mapping session.

```
port-mapping session_id {enable | disable}
no port-mapping session_id
```

**Syntax Definitions**

- `session_id`: The port mapping session ID.
- `enable`: Enables a port mapping session.
- `disable`: Disables a port mapping session.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To be enabled, a session should have a minimum of two ports.

**Examples**

```
-> port-mapping 3 enable
-> port-mapping 4 disable
-> no port-mapping 5
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- `port-mapping user-port network-port`: Creates a port mapping session with or without the user ports, network ports, or both.
- `port-mapping unidirectional bidirectional`: Configures the direction of a port mapping session.
- `show port-mapping status`: Displays the status of one or more port mapping sessions.
- `show port-mapping`: Displays the configuration of one or more port mapping sessions.

MIB Objects

PortMappingSessionTable
  - pmapSessionNumber
  - pmapSessionStatus
port-mapping unidirectional bidirectional

Configures the direction of a port mapping session.

```
port-mapping session_id [unidirectional | bidirectional]
```

**Syntax Definitions**

- `session_id`: The port mapping session ID.
- `unidirectional`: Specifies unidirectional port mapping.
- `bidirectional`: Specifies bidirectional port mapping.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>unidirectional</td>
<td>bidirectional</td>
</tr>
</tbody>
</table>

**Platform Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- In the bidirectional mode, the network ports of a session cannot communicate with each other. Also, the network ports of that session cannot be a part of a network port set of another session.

- In the unidirectional mode, the network ports of a session can communicate with each other. Also, the network ports of that session can be part of a network port set of another session that is in the unidirectional mode.

- To change the directional mode of an active session with network ports, delete the network ports of the session, change the direction, and recreate the network ports.

**Examples**

```
-> port-mapping 5 enable unidirectional
-> port-mapping 5 disable unidirectional
-> port-mapping 6 enable bidirectional
-> port-mapping 5 disable bidirectional
```
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `port-mapping user-port network-port`  
  Creates a port mapping session with or without the user ports, network ports or both.
- `port-mapping`  
  Enables, disables, or deletes a port mapping session.
- `show port-mapping`  
  Displays the configuration of one or more port mapping sessions.

**MIB Objects**

- `PortMappingSessionTable`
- `PmapSessionNumber`
- `PmapSessionDirection`
**port-mapping unknown-unicast-flooding**

Enables or disables flooding of unicast traffic from all the switch ports to the user ports related to a particular session.

```
port-mapping session_id unknown-unicast-flooding {enable | disable}
```

**Syntax Definitions**

- `session_id`: The port mapping session ID.
- `enable`: Enables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.
- `disable`: Disables the flooding of unknown unicast traffic from all ports to the user ports for a particular session.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platform Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Configuring unknown unicast flooding creates a new port mapping session if there is no existing session.
- When a link aggregate is configured as a user port, the unknown unicast flooding configuration is applied to all the member ports of the aggregate.

**Examples**

```
-> port-mapping 1 unknown-unicast-flooding enable
-> port-mapping 2 unknown-unicast-flooding disable
```

**Release History**

Release 7.1.1; command introduced.
**Related Commands**

- `port-mapping user-port network-port`
  Creates a port mapping session with or without the user ports, network ports or both.
- `port-mapping`
  Enables, disables, or deletes a port mapping session.
- `show port-mapping`
  Displays the configuration of one or more port mapping sessions.
- `show port-mapping status`
  Displays the status of one or more port mapping sessions.

**MIB Objects**

- `portMappingSessionTable`
  - `pmapSessionUnknownUnicastFloodStatus`
**port-mapping dynamic-proxy-arp**

Enables or disables the dynamic proxy ARP functionality for the port mapping session.

```
port-mapping session_id dynamic-proxy-arp {enable | disable}
```

**Syntax Definitions**

- **session_id**: The port mapping session for which the dynamic proxy ARP status is enabled or disabled.
- **enable**: Enables the dynamic proxy ARP status.
- **disable**: Disables the dynamic proxy ARP status.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td>No</td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td>No</td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td>No</td>
</tr>
<tr>
<td>X24C2</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Clients must be connected to the user-ports and the head end routers connected to the network-ports of the port mapping session for dynamic proxy ARP to function properly.
- DHCP snooping must be enabled for dynamic proxy ARP to function.
- Using dynamic proxy ARP in conjunction with DHCP snooping allows for the configuration of the MAC Forced Forwarding feature.
- When dynamic proxy ARP is enabled, port-group allocation will be triggered. The TCAM manager will respond as success if the port-group allocation is a success. If QoS is already using the port-groups, the TCAM manager will respond with a failure and an error is displayed.
- Dynamic proxy ARP can be enabled on only two port-groups. If QoS is already using the port-groups, an error message is displayed.

**Examples**

- `-> port-mapping 1 dynamic-proxy-arp enable`
- `-> port-mapping 1 dynamic-proxy-arp disable`
**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **port-mapping user-port network-port**: Creates a port mapping session with or without the user ports, network ports or both.
- **port-mapping**: Enables, disables, or deletes a port mapping session.
- **show port-mapping**: Displays the configuration of one or more port mapping session.
- **show port-mapping status**: Displays the status of one or more port mapping session.
- **show ip dynamic-proxy-arp**: Displays the ARPs learned through dynamic proxy.

**MIB Objects**

- portMappingSessionTable
- pmapSessionDynProxyARP
**show port-mapping status**

Displays the status of one or more port mapping sessions.

```
show port-mapping [session_id] status
```

### Syntax definitions

- **session_id**
  
  The port mapping session ID.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If you do not specify the port mapping session ID, then the status of all the port mapping sessions are displayed.

### Examples

```
$ -> show port-mapping status

SessionID  Direction Status Unknown Unicast DPA Status
----------+-------------------+-----------------+----------------+---------------
     1  bi       disable flood enable
     1  bi       enable drop disable
     2  bi       disable flood disable
```

### Output definitions

- **SessionID**
  
  Displays the port mapping session ID.

- **Direction**
  
  Displays the direction of a port mapping session.

- **Status**
  
  Displays status of a port mapping session.

- **Unknown Unicast**
  
  Whether unknown unicast traffic is dropped or flooded from all the switch ports to the user ports related to the port mapping session.

- **DPA Status**
  
  Displays the status of Dynamic Proxy ARP for the port mapping session. This functionality is supported only on the OmniSwitch 6465 and OmniSwitch 6865.
**Release History**

Release 7.1.1; command introduced.
Release 8.6R1; “DPA Status” field added.

**Related Commands**

- **port-mapping user-port**  
  Creates a port mapping session with or without the user ports, network ports, or both.

- **network-port**

- **port-mapping**  
  Enables, disables, or deletes a port mapping session.

**MIB Objects**

PortMappingSessionTable

- PmapSessionNumber
- PmapSessionDirection
- pmapSessionStatus
- pmapSessionUnknownUnicastFloodStatus
- pmapSessionDynProxyARP
**show port-mapping**

Displays the configuration of one or more port mapping sessions.

`show port-mapping [session_id]`

---

**Syntax Definitions**

- **session_id**
  The port mapping session ID.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you do not specify the port mapping session ID, then the user port and network port information are displayed for all the port mapping sessions active on the switch.

**Examples**

```
-> show port-mapping 3
```

**output definitions**

- **SessionID**
  Displays the port mapping session ID.

- **USR-PORT**
  Displays the set of user ports of a port mapping session.

- **NETWORK-PORT**
  Displays the set of network ports of a port mapping session.

**Release History**

Release 7.1.1; command introduced.
Related Commands

```
port-mapping user-port
network-port

port-mapping
```

Creates a port mapping session with or without the user ports, network ports, or both.

Enables, disables, or deletes a port mapping session.

MIB Objects

```
PortMappingSessionTable
  PmapSessionNumber
PortMappingTable
  pmapPortIfindex
  pmapPortType
```
show ip dynamic-proxy-arp

Displays the ARPs learned through dynamic proxy.

show ip dynamic-proxy-arp

Syntax definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
- This command shows the information related to the router IP.
- To view the output, dynamic proxy must be enabled on the port mapping session, DHCP snooping must be enabled on the VLAN.

Examples

-> show ip dynamic-proxy-arp

<table>
<thead>
<tr>
<th>Router IP Addr</th>
<th>Hardware Addr</th>
<th>Vlan</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.35.3</td>
<td>e9:ca:ab:e3:23:4c</td>
<td>500</td>
<td>1/1/23</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Router IP Addr</th>
<th>Displays the IP address of the router learned through option-3 in DHCPACK message.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Addr</td>
<td>Displays the MAC address of the router.</td>
</tr>
<tr>
<td>Vlan</td>
<td>Displays the VLAN associated with the router.</td>
</tr>
<tr>
<td>Interface</td>
<td>The exact interface on which the router IP was learned.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.
Port Mapping Commands

show ip dynamic-proxy-arp

Related Commands

port-mapping dynamic-proxy-arp  Enables or disables the dynamic proxy ARP functionality for the port mapping session.

MIB Objects

alaIpNetToMediaDpaIp
alaIpNetToMediaDpaPhysAddress
alaIpNetToMediaDpaChassisId
alaIpNetToMediaDpaSlot
alaIpNetToMediaDpaPort
Learned Port Security (LPS) provides a mechanism for controlling network device communication on one or more switch ports. Configurable LPS parameters allow the user to restrict source learning on a port to:

- A maximum number of learned source MAC addresses.
- A specific amount of time in which source MAC addresses are learned.
- An individual learned source MAC address.
- A range of learned source MAC addresses.

This chapter includes descriptions of the CLI commands used to define LPS parameters and display information about the current LPS configuration.

MIB information for Learned Port Security commands is as follows:

- **Filename**: ALCATEL-IND1-LPS-MIB.mib
- **Module**: alcatelIND1LearnedPortSecurityMIB

A summary of the available commands is listed here:

```
port-security
port-security learning-window
port-security convert-to-static
port-security mac
port-security maximum
port-security port max-filtering
port-security mac-range
port-security port violation
port-security learn-trap-threshold
port-security port pkt-relay
port-security pkt-relay protocol
port-security pkt-relay protocol udp
show port-security pkt-relay filter
show port-security
show port-security mac-range
show port-security brief
show port-security learning-window
```
port-security

Enables or disables Learned Port Security (LPS) on the switch port(s) or SAP. When LPS is enabled, only devices that have a source MAC address that complies with LPS restrictions are learned on the port(s).

\[ \text{port-security \{port }\text{ chassis/slot/port[-port2] | chassis} | \{ \text{sap }\text{ port | linkagg} \text{ sap_id} \} \text{ [admin-state} \{ \text{enable | disable | locked}\} \] 

\[ \text{no port-security }\{\text{port }\text{ chassis/slot/port[-port2] | sap} \text{ port | linkagg} \text{ sap_id}\} \]

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **chassis**
  - Specifies all LPS ports.

- **sap_id**
  - The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*

- **enable**
  - Administratively enables LPS on the specified port(s).

- **disable**
  - Administratively disables LPS on the specified port(s). All bridged and filtered MAC addresses are cleared, but the static MAC address and LPS configuration for the port is retained. Learning is unrestricted.

- **locked**
  - Administratively disables all learning on the port. Existing MAC addresses are retained but no additional learning of addresses, except for static MAC addresses, is allowed.

**Defaults**

By default, LPS functionality is disabled on all ports.

The following default value applies if the **admin-state** parameter is *not* specified with this command:

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-state</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the `no` form of this command to remove the LPS configuration from the specified port and clear all MAC addresses learned on the port. Note that the `chassis` parameter is not supported when using the `no` form of this command.

- The `admin-state disable` option disables LPS on the port but does not clear the LPS configuration.

- Use the `chassis` parameter to administratively disable or enable all active LPS ports with one command. This option does not apply to ports on which LPS was not previously enabled.

- LPS is supported on Ethernet fixed, 802.1Q-tagged ports, and access ports.

- LPS is not supported on link aggregates, 802.1Q tagged (trunked) link aggregates, or link aggregate member ports.

- Note that when LPS is enabled on an active port, all MAC addresses previously learned on that port are cleared from the source learning MAC address table.

- LPS is also supported on ports that have Universal Network Profile (UNP) functionality enabled, with the following conditions:
  - When LPS is enabled or disabled on a UNP bridge port (LPS is not supported on UNP access ports), MAC addresses already learned on that port are flushed.
  - UNP authentication and classification is applied first, then LPS rules.
  - If UNP classifies a MAC address as forwarding but LPS learns the address as filtering, an untagged packet will show as filtering in the default VLAN for the port and a tagged packet MAC will show as filtering in the specific tagged VLAN.
  - When a MAC address is filtered by LPS, the `show unp user status` command will display “LPS-B” as the profile classification source for that MAC address.

- LPS allows for the configuration of the following source MAC address learning restrictions:
  - A source learning time limit window to specify the length of time learning is allowed on a port.
  - A maximum number of bridged and filtered MAC addresses allowed on a specific port
  - A list of MAC addresses (individual or range of addresses) allowed on a port.
  - How a port handles traffic that is unauthorized.

Examples

- `port-security port 4/8 admin-state enable`
- `port-security port 2/1-10 admin-state enable`
- `port-security chassis admin-state disable`
- `no port-security port 1/1-12`
- `port-security sap port 2/1/10:10`
- `port-security sap port 2/1/10:10.20`
- `port-security sap linkagg 10:10`
- `port-security sap linkagg 10:20`
- `no port-security sap port 2/1/10:10`
- `no port-security sap linkagg 10:20`

Release History

Release 7.1.1; command introduced.
Release 8.8R1; `sap` parameter added.
Related Commands

**port-security mac-range**  Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.

**port-security maximum**  Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

**port-security learning-window**  Configures the amount of time, in minutes, to allow source learning on all LPS ports.

**port-security port violation**  Selects the method for handling traffic that does not comply with LPS restrictions for the specified port(s).

MIB Objects

learnedPortSecurityTable  
   lpsAdminStatus

learnedPortSecuritySAPTable  
   lpsSAPAdminStatus
port-security learning-window

Configures the amount of time, in minutes, to allow source learning on all LPS ports. This LPS parameter applies to the entire switch, so when the time limit expires, source learning of new MAC addresses is stopped on all LPS ports. Only authorized MAC addresses are allowed to be associated on LPS ports after this timer expires. This command also enables or disables the conversion of dynamic MAC addresses to static MAC addresses on LPS ports.

```
port-security learning-window minutes [convert-to-static {enable | disable}] [no-aging {enable | disable}] [mac-move {enable | disable}] [learn-as-static {enable | disable}] [boot-up {enable | disable}]
```

Syntax Definitions

- `minutes` The number of minutes during which LPS allows source learning across all LPS ports. This amount of time defines the LPS learning window. The valid range is 0–2880. When this value is set to zero, the learning window time is set to infinity (no source learning time restriction on LPS ports).

- `convert-to-static enable` Enables the `convert-to-static` option for the learning window. Dynamically learned bridged (not filtered) MAC addresses are automatically converted to static addresses when the learning window closes. This option is automatically disabled when the LPS learning window is set to infinity (zero).

- `convert-to-static disable` Disables the `convert-to-static` option for the learning window. Dynamically learned bridged MAC addresses are not converted to static addresses and will start to age out when the learning window closes.

- `no-aging enable` Enables the `no-aging` option for the learning window. Dynamically learned bridged MAC addresses are learned as `pseudo-static` MACs, which do not age out but are not saved in the switch configuration. MAC movement is not allowed for pseudo-static MAC addresses unless the `mac-move` option is also enabled.

- `no-aging disable` Disables the `no-aging` option for the learning window. MAC addresses are learned as dynamic addresses that will age out.

- `mac-move enable` Enables the `mac-move` option. Allows a pseudo-static MAC address to move to a different port in the same VLAN without getting dropped. The `mac-move` option is used with the `no-aging` option to allow MAC movement for pseudo-static MAC addresses.

- `mac-move disable` Disables the `mac-move` option. If the `no-aging` option is enabled, MAC movement for pseudo-static MAC addresses is not allowed. Frames from a duplicate pseudo-static MAC address are dropped.

- `learn-as-static enable` Enables the `learn-as-static` option for the learning window. Dynamically learned bridged MAC addresses are converted to permanent static MAC addresses during the learning window time (even if the `convert-to-static` option is disabled). MAC movement is allowed for the permanent static MAC addresses. This option and the `no-aging` option are mutually exclusive.
Learned Port Security Commands

Defaults

By default, the LPS source learning time limit is not set for the switch; the learning window defaults to infinity (source learning is not limited to a specific time frame).

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>convert-to-static</td>
<td>disable</td>
</tr>
<tr>
<td>no-aging</td>
<td>disable</td>
</tr>
<tr>
<td>mac-move</td>
<td>disable</td>
</tr>
<tr>
<td>learn-as-static</td>
<td>disable</td>
</tr>
<tr>
<td>boot-up</td>
<td>enable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to clear the learning window time (no learning window time limit is applied to the port).

- The LPS source learning time window is started and/or reset each time the port-security learning-window command is issued or when the port-security learning-window boot-up option is enabled and the switch restarts.

- Setting the LPS learning window time to 0 (zero) configures an infinite source learning time period for all LPS ports. The learning of MAC addresses on LPS ports never times out.

- When the LPS learning window time is set to zero, all options except the convert-to-static option are still valid. For example, the no-aging option setting still applies.

- After the LPS learning window time expires, MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of bridged MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.
• Enabling the no-aging option triggers the following LPS learning window behavior:
  – All new bridged MAC addresses are learned as pseudo-static MAC addresses during the learning
  window time period. Pseudo-static addresses do not age out but are not saved to the switch
  configuration.
  – MAC movement is not allowed for pseudo-static MAC addresses unless the mac-move option is
  also enabled. The mac-move status (enabled or disabled) applies only to the no-aging option.
  – Enabling the mac-move option is not allowed unless the no-aging option is also enabled. When the
  mac-move option is enabled, disabling the no-aging option is not allowed.
  – When the learning window starts, any MAC addresses that were learned prior to the learning
  window time period are retained as dynamic addresses; they are not converted to pseudo-static
  MAC addresses.

• The learn-as-static and no-aging options are mutually exclusive; if both are enabled, then the learn-
  as-static option takes precedence.

• If the convert-to-static option is enabled, then all dynamic bridged and pseudo-static MAC addresses
  are converted to static MAC addresses when the learning window closes. Static MAC addresses do not
  age out and are saved to the switch configuration.

Note. When UNP is enabled on any one LPS port, the convert-to-static, no-aging, and boot-up
parameter options are not supported on all LPS-enabled ports. This is because the learning window
configuration is global and applies to all LPS ports.

Examples
-> port-security learning-window 25
-> port-security learning-window 2 convert-to-static enable
-> port-security learning-window 60 no-aging enable mac-move enable
-> port-security learning-window 0 learn-as-static enable
-> port-security learning-window 500 boot-up disable
-> port-security learning-window 2 convert-to-static enable no-aging enable
-> port-security learning-window 2 no-aging enable convert-to-static enable boot-up
  enable learn-as-static enable mac-move enable
-> no port-security learning-window

Release History
Release 7.1.1; command introduced.
Release 7.2.1.R02; no-aging and boot-up parameters added.
Release 8.2.1; learn-as-static and mac-move parameters added.
Learned Port Security Commands

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port-security</strong></td>
<td>Enables or disables Learned Port Security (LPS) on the switch port(s).</td>
</tr>
<tr>
<td><strong>port-security maximum</strong></td>
<td>Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.</td>
</tr>
<tr>
<td><strong>port-security port maximum</strong></td>
<td>Configures the maximum number of MAC addresses that can be filtered on the LPS port.</td>
</tr>
<tr>
<td><strong>port-security port violation</strong></td>
<td>Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.</td>
</tr>
<tr>
<td><strong>show port-security learning-window</strong></td>
<td>Displays the source learning window configuration.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- `learnedPortSecurityGlobalGroup`
  - `lpsLearningWindowTime`
  - `lpsLearningWindowTimeWithStaticConversion`
  - `lpsLearningWindowNoAging`
  - `lpsLearningWindowBootupStatus`
  - `lpsLearningWindowLearnAsStatic`
  - `lpsLearningWindowPseudoMacMove`
**port-security convert-to-static**

Converts all MAC addresses dynamically learned on the LPS port(s) to static MAC addresses. This command does not apply to MAC addresses that are filtered.

```
port-security {port chassis/slot/port[-port2] | chassis} | {sap {port | linkagg} sap_id} convert-to-static
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **chassis**
  - Specifies all the LPS ports on the chassis.

- **sap_id**
  - The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Converting dynamic MAC addresses to static MAC addresses is not supported on Universal Network Profile (UNP) ports.

- You can stop the aging out of dynamic MAC addresses on the LPS port(s) by converting them to static MAC addresses.

- The number of converted static MAC addresses cannot exceed the maximum number of MAC addresses allowed on the port(s).

**Note.** The **port-security convert-to-static** command is not supported on UNP ports.

**Examples**

- `-> port-security port 4/8 convert-to-static`
- `-> port-security chassis convert-to-static`
- `-> port-security sap port 2/1/10:10 convert-to-static`
Learned Port Security Commands

**Release History**
Release 7.2.1.R02; command was introduced.
Release 8.8R1; sap parameter added.

**Related Commands**
- `port-security` Enables or disables Learned Port Security (LPS) on the switch port(s).
- `port-security maximum` Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

**MIB Objects**
- `learnedPortSecurityGlobalGroup`
- `lpsConvertToStatic`
- `learnedPortSecuritySAPTable`
- `lpsSAPConvertToStatic`
**port-security mac**

Configures a static MAC address on the specified LPS port. This command also enables LPS on the specified port, if LPS is not already active on the port.

```
port-security {port chassis/slot/port[-port2] | sap {port | linkagg} sap_id} mac mac_address [vlan vlan_id]
```

```
no port-security {port chassis/slot/port[-port2] | sap {port | linkagg} sap_id} mac [all | mac_address] [vlan vlan_id]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `sap_id` The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*
- `mac_address` MAC address to configure as a static MAC address on the specified LPS port (for example, 00:20:95:00:10:2A).
- `vlan` The VLAN ID to associate with the specified LPS port.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove a specific static MAC address or all of the static MAC addresses configured on the specified LPS port. Note that even when all statically configured MAC addresses are removed, LPS remains active on the port.

- A VLAN-port association (VPS) must exist between the specified VLAN and the LPS port. If no VLAN ID is specified with this command, the default VLAN for the LPS port is used.

- The following conditions will display an error or warning message:
  - A VLAN ID is specified that is not associated with the LPS port:
  - An attempt is made to configure a MAC address more than once on the same LPS port with the
Learned Port Security Commands

- A duplicate MAC address is configured on different LPS ports.

- Configuring a multicast MAC address, an all zero MAC address, or a broadcast MAC address is not allowed with this command.

- Use this command instead of the `mac-learning static mac-address` command to create a static MAC address on an LPS port.

**Examples**

```
-> port-security port 1/1/20 mac 00:20:95:00:fa:5c
-> port-security port 1/1/1-15 mac 00:da:95:00:00:10
-> no port-security port 1/1/20 mac 00:20:95:00:fa:5c
-> no port-security port 1/1/1-15 mac 00:da:95:00:00:10

-> port-security port 1/1/20 mac 00:2a:95:11:22:10 vlan 200
ERROR: Vlan 200 is not valid on this port

-> port-security port 1/1/20 mac 00:2a:95:11:22:10 vlan 200
ERROR: Mac 00:2a:95:11:22:10 ALREADY exists on Vlan 200 for port 1/1/20

```

**Release History**

Release 8.4.1; command introduced.
Release 8.8R1; `sap` parameter added.
Related Commands

- **port-security**
  Enables or disables Learned Port Security (LPS) on the switch port(s).

- **port-security learning-window**
  Configures the amount of time in minutes to allow source learning on all LPS ports.

- **port-security maximum**
  Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

- **port-security port max-filtering**
  Configures the maximum number of MAC addresses that can be filtered on the LPS port.

- **port-security port violation**
  Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

- **show port-security pkt-relay filter**
  Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

- **learnedPortSecurityAgL2MacAddressTable**
  - lpsAgL2MacAddress
  - lpsAgL2VlanId
  - lpsAgL2MacAddressRowStatus

- **learnedPortSecuritySAPTable**
  - lpsSAPL2HighMacAddress
  - lpsSAPL2LowMacAddress
**port-security maximum**

Specifies the maximum number of bridged MAC addresses that an LPS port(s) is allowed to learn.

```
port-security {port chassis/slot/port[-port2] | sap {port | linkagg} sap_id} maximum number
```

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **sap_id**
  - The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*

- **number**
  - The number of source MAC addresses that are allowed on this port. The valid range is 1–1000.

**Defaults**

By default, the number of MAC addresses allowed is set to 1.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Any additional source MAC addresses received that exceed the maximum number of bridged addresses allowed are filtered on the port, regardless of the LPS learning window time limit. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.

- Note that source learning of configured authorized MAC addresses is still allowed after the LPS time limit has expired; however, all learning is stopped if the number of MAC addresses learned meets or exceeds the maximum number of addresses allowed, even if the LPS time limit has not expired.

**Examples**

```
-> port-security port 2/14 maximum 25
-> port-security port 4/10-15 maximum 100
-> port-security sap port 2/1/10:10.20 maximum 50
-> port-security sap linkagg 10:10 maximum 500
```
**Release History**

Release 7.1.1; command introduced.  
Release 8.8R1; **sap** parameter added.

**Related Commands**

- `port-security` Enables or disables Learned Port Security (LPS) on the switch port(s).
- `port-security learning-window` Configures the amount of time in minutes to allow source learning on all LPS ports.
- `port-security learn-trap-threshold` Configures the number of bridged MAC addresses to learn before sending a SNMP trap.
- `port-security port violation` Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

**MIB Objects**

- `learnedPortSecurityTable`  
  - `lpsMaxMacNum`
- `learnedPortSecuritySAPTable`  
  - `lspSAPMaxMacNum`
Learned Port Security Commands

**port-security learn-trap-threshold**

Configures the number of bridged MAC addresses to learn before sending a SNMP trap.

```
port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} learn-trap-threshold number
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port[-port2]` The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `sap_id` The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*
- `number` The number of bridged MAC addresses to learn before sending a trap. The valid range is 0–1000.

**Defaults**

By default, the number of bridged MAC addresses to learn before sending a trap is set to the same value as the maximum number of bridged MAC addresses allowed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the number of bridged MAC addresses learned on the port matches the specified threshold amount, a trap is sent for every bridged MAC address learned thereafter.

- Sending a trap when this threshold is reached provides notification of newly learned bridged MAC addresses. Trap contents includes identifying information about the MAC, such as the address itself, the corresponding IP address, switch identification, and the slot and port number on which the MAC was learned.

- If this threshold value is set to zero, a trap is sent for every MAC address learned on the LPS port.

**Examples**

```
-> port-security port 1/10 learn-trap-threshold 6
-> port-security port 1/10-13 learn-trap-threshold 18
-> port-security sap port 2/1/10:10 learn-trap-threshold 1
```
**Release History**

Release 7.1.1; command introduced.
Release 8.8R1; sap parameter added.

**Related Commands**

- **port-security maximum** Configures the maximum number of source MAC addresses that an LPS port is allowed to learn.
- **show port-security pkt-relay filter** Displays Learned Port Security (LPS) configuration and table entries.

**MIB Objects**

- `learnedPortSecurityTable` `lpsLearnTrapThreshold`
- `learnedPortSecuritySAPTable` `lpsSAPlearnTrapThreshold`
**port-security port max-filtering**

Configures the maximum number of MAC addresses that can be filtered on the LPS port(s).

```
port-security {port chassis/slot/port[-port2] | sap {port | linkagg} sap_id} max-filtering number
```

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port[-port2]`: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
- `sap_id`: The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*
- `number`: The maximum number of filtered MAC addresses that are allowed on this port. The valid range is 0–100.

**Defaults**

By default, the maximum number of MAC addresses that can be filtered on an LPS port is 5.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the number of filtered MAC addresses learned on the port reaches the maximum, the violation mode (restrict, discard, or shutdown) configured for the port is applied.

- Any additional source MAC addresses received that exceed the maximum number of bridged addresses allowed are filtered on the port, regardless of the LPS learning window time limit. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.

- Even after the LPS learning window time expires, MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.

**Examples**

```
-> port-security port 1/10 max-filtering 6
-> port-security port 1/10-13 max-filtering 18
```
Learned Port Security Commands

- port-security sap port 2/1/10:10 max-filtering 100
- port-security sap port 2/1/10:10.20 max-filtering 50
- port-security sap linkagg 10:10 max-filtering 25
- port-security sap linkagg 10:20 max-filtering 5

Release History
Release 7.1.1; command introduced.
Release 8.8R1; sap parameter added.

Related Commands

port-security maximum
Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

port-security learning-window
Configures the amount of time in minutes to allow source learning on all LPS ports.

port-security port violation
Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

show port-security pkt-relay
Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

learnedPortSecurityTable
  lpsMaxFilteredMacNum
learnedPortSecuritySAPTable
  lpsSAPMaxFilteredMacNum
**port-security mac-range**

Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port. This command also enables LPS on the specified port, if LPS is not already active on the port.

```
port-security [port chassis/slot/port[-port2] | sap {port | linkagg} sap_id] mac-range [low mac_address | high mac_address]
```

```
no port-security {port chassis/slot/port[-port2] | sap {port | linkagg} sap_id} mac-range [low mac_address]
```

---

**Syntax Definitions**

- `chassis/slot/port[-port2]` The chassis, slot and port number (1/1/1). Use a hyphen to specify a range of ports (1/1/1-8). On the OmniSwitch 6900 only, configuring multiple MAC address ranges for the same port is supported.

- `sap_id` The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*

- `low mac_address` MAC address that defines the low end of a range of MACs (for example, 00:20:95:00:10:2A).

- `high mac_address` MAC address that defines the high end of a range of MACs (for example, 00:20:95:00:10:2F).

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>high mac_address</td>
<td>ff:ff:ff:ff:ff:ff</td>
</tr>
<tr>
<td>low mac_address</td>
<td>00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- By default, each LPS port is set to a range of 00:00:00:00:00:00–ff:ff:ff:ff:ff:ff, which includes all MAC addresses.

- Source MAC addresses received on an LPS port that fall within the authorized range are allowed on the port. An additional entry is made in the LPS table for each of these learned addresses.
Any additional source MAC addresses received that do not match the configured authorized addresses are not allowed (filtered) on the port, regardless of the LPS learning window time limit or the maximum number of bridged addresses allowed. Once the number of filtered MAC addresses reaches the maximum number of filtered addresses allowed, the port violation mode is applied.

Configuring more than one MAC address range per port is supported. When attempting to configure multiple MAC address ranges on the same port, consider the following:

- A maximum of eight multiple MAC address ranges can be configured per port.
- On a newly configured LPS port, the first user configured MAC range would overwrite the default MAC range.
- A MAC range cannot overlap with another MAC range configured for the port.
- Modifying a MAC range is allowed only if the lower MAC address is not changed and the defined new range does not overlap with the existing range. To modify the lower MAC address, the existing range must be deleted before adding the new range.
- When modifying a MAC range, the new range must match or accommodate any existing static MACs on the port, else an error will be thrown indicating some static MACs exist on the port that fall outside the new/resultant MAC range being configured. (Note: It is required to flush such static MACs on the port, if user needs to configure the new MAC range, which was not accommodating the static MACs).
- When the MAC range size is increased, all the dynamic filtering MACs on the port would be flushed.
- When the MAC range size is reduced, any existing dynamic forwarding MACs learned on the port would be flushed if they fall outside any MAC ranges configured on the port at that point of time.
- All the dynamic filtering MACs learned on the port would be flushed.

Use the no form of this command to delete the configured MAC range.

The default MAC range is automatically applied when all the configured MAC ranges for the port are deleted.

The default MAC range on the port cannot be deleted.

Examples

- `port-security port 1/5/11-15 mac-range low 00:da:95:00:00:10 high 00:da:95:00:00:1f`
- `port-security port 1/1/5 mac-range low 00:01:01:22:22:56 high 00:01:01:22:22:67`
- `port-security port 1/1/5 mac-range low 00:01:01:22:33:56 high 00:01:01:22:33:67`
- `port-security port 1/1/5 mac-range low 00:01:01:22:44:56 high 00:01:01:22:44:67`
- `no port-security port 1/1/5 mac-range low 00:01:01:22:33:56`

Release History

Release 7.1.1; command introduced.
Release 8.5R3; ability to configure multiple MAC ranges per port added.
Release 8.8R1; sap parameter added.
Related Commands

- **port-security**
  Enables or disables Learned Port Security (LPS) on the switch port(s).

- **port-security learning-window**
  Configures the amount of time in minutes to allow source learning on all LPS ports.

- **port-security maximum**
  Specifies the maximum number of source MAC addresses that an LPS port(s) is allowed to learn.

- **port-security port max-filtering**
  Configures the maximum number of MAC addresses that can be filtered on the LPS port.

- **port-security port violation**
  Selects the method for handling traffic that does not comply with LPS restrictions for the specified port.

- **port-security port pkt-relay**
  Displays the LPS configuration and table entries.

- **show port-security mac-range**
  Displays the MAC ranges configured on the LPS ports.

MIB Objects

learnedPortSecurityTable
  - lpsLoMacRange
  - lpsHiMacRange
  - lpsRowStatus

learnedPortSecurityL2MacRangeTable
  - lpsL2LowMacAddress
  - lpsL2HighMacAddress
**port-security port violation**

Selects the method for handling traffic that does not comply with LPS restrictions for the specified port(s).

```
port-security {port chassis/slot/port|-port2} | sap {port | linkagg} sap_id} violation {shutdown | restrict | discard} | violation recovery-time {default | seconds} | violation recovery-maximum {infinite | default | max_attempts}
```

**Syntax Definitions**

- **chassis**
  The chassis identifier.

- **slot/port[-port2]**
  The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).

- **sap_id**
  The SAP ID number identifying the service instance. *This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.*

- **shutdown**
  The port is administratively disabled when the port receives unauthorized traffic. No further traffic is allowed on the port.

- **restrict**
  Filters (blocks) unauthorized traffic but allows traffic that complies with LPS restrictions to forward on the port. The port remains administratively enabled.

- **discard**
  Disables learning on the port when unauthorized traffic is received or the configured maximum number of MAC addresses is reached. The port remains administratively enabled.

- **default**
  Sets the SAP recovery-time or recovery-maximum values to their default setting.

- **seconds**
  The number of seconds after which the SAP is reactivated. The valid range is 30-600 seconds.

- **infinite**
  Sets the recovery attempts to infinite for a SAP.

- **max_attempts**
  The maximum number of recovery attempts. Valid range is 0-50.

- **clear**
  Clears the violation on a SAP.

**Defaults**

By default, the security violation mode is set to restrict when LPS is enabled on the port.

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>violation</td>
<td>restrict</td>
</tr>
<tr>
<td>seconds</td>
<td>300 seconds</td>
</tr>
<tr>
<td>max_attempts</td>
<td>10</td>
</tr>
</tbody>
</table>
**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When a traffic violation occurs on an LPS port, a notice is sent to the switch log.
- If the violation mode is set to `restrict`, unauthorized source MAC addresses are not learned in the LPS table, but they are recorded in the source learning MAC address table with a filtered operational status. This allows the user to view MAC addresses attempting unauthorized access to the LPS port.
- Only violation mode `restrict` is supported on a SAP.

**Examples**

- `port-security port 2/14 violation restrict`
- `port-security port 4/10-15 violation shutdown`
- `port-security port 1/37 violation discard`
- `port-security sap port 2/1/10:10 violation recovery-maximum 4`
- `port-security sap port 2/1/10:10.20 violation recovery-time 60`
- `port-security sap linkagg 10:10 violation restrict`
- `port-security sap linkagg 10:20 violation clear`

**Release History**

Release 7.1.1; command introduced.
Release 7.2.1.R02; `discard` parameter added.
Release 8.8R1; `sap` parameter added.

**Related Commands**

- `port-security` Enables or disables Learned Port Security (LPS) on the switch port(s).
- `clear violation` Clears all port violations; allows the port to resume normal operation without a manual reset of the port or module.
- `show port-security` Displays Learned Port Security (LPS) configuration and table entries.

**MIB Objects**

- `learnedPortSecurityTable`
- `lpsViolationOption`
- `learnedPortSecuritySAPTable`
- `lpsSAPViolationRecoveryMax`
- `lpsSAPViolationRecoveryTime`
- `lpsSAPViolationRestrict`
- `lpsSAPViolationClear`
**port-security port pkt-relay**

Enables packet relay feature on a single or range of LPS ports.

```
port-security {port chassis/slot/port[-port2]} pkt-relay
no port-security {port chassis/slot/port[-port2]} pkt-relay
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port[-port2]**
  - The slot and port number. Use a hyphen to specify a range of ports.

### Defaults

By default, the packet relay is disabled on LPS port.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When packet relay is enabled on a non LPS port, the LPS is automatically enabled on that port.
- Packet relay feature is not supported on UNP ports.
- Use the `no` form of the command to disable packet relay on the port.

### Examples

```
-> port-security port 3/2/1 pkt-relay
-> port-security port 3/2/1-4 pkt-relay
-> no port-security port 3/2/1-4 pkt-relay
```

### Release History

Release 8.8R2; command introduced.
Related Commands

- **port-security pkt-relay**
  - **protocol**
  - **show port-security pkt-relay**
  - **filter**

  Configures the protocol filter criteria for packet relay feature.

  Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

- **lpsPacketRelay**
Learned Port Security Commands

port-security pkt-relay protocol

Configures the protocol filter criteria for packet relay feature.

port-security pkt-relay protocol {udp} {icmp} {igmp}

Syntax Definitions

udp
The packets with UDP protocol are considered for retransmission to the queue.

icmp
The packets with ICMP protocol are considered for retransmission to the queue.

igmp
The packets with IGMP protocol are considered for retransmission to the queue.

Defaults
By default, no protocol is enabled as filter for packet relay.

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When the protocol filter is configured, it is applied on all the ports on which packet relay is enabled.
- More than one protocol can be configured for protocol filter.

Examples

-> port-security pkt-relay protocol udp
-> port-security pkt-relay protocol icmp igmp

Release History

Release 8.8R2; command introduced.
Related Commands

```
port-security pkt-relay protocol udp
```

Configures the UDP source and destination ports as the criteria for packet relay.

MIB Objects

```
lpsPacketRelay
  lpsPacketRelayUdpStatus
  lpsPacketRelayIgmpStatus
  lpsPacketRelayIcmpStatus
```
**port-security pkt-relay protocol udp**

Configures the UDP source and destination ports as the criteria for packet relay.

`port-security pkt-relay protocol udp [src-port \[port1[-port2]\]] [dst-port \[port1[-port2]\]]`

---

**Syntax Definitions**

- **src-port**
  Specify the UDP source port for packet relay.

- **dst-port**
  Specify the UDP destination port for packet relay.

- **port1**
  Specify the port number which will be matched for retransmission to the queue.

- **port2**
  Specify the port range for sequential port.

---

**Defaults**

By default, no UDP source and destination ports are configured for packet relay.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use this command to specify a particular or range of UDP source and destination port for packet relay.

- UDP protocol filter must be configured before configuring specific UDP source and destination ports. Use the `port-security pkt-relay protocol` CLI.

---

**Examples**

- `-> port-security pkt-relay protocol udp src-port 2`
- `-> port-security pkt-relay protocol udp src-port 2-6`
- `-> port-security pkt-relay protocol udp dst-port 4`
- `-> port-security pkt-relay protocol udp dst-port 4-6`

---

**Release History**

Release 8.8R2; command introduced.
Related Commands

- **port-security pkt-relay protocol**
  Configures the protocol filter criteria for packet relay feature.

- **port-security port pkt-relay**
  Enables packet relay feature on a single or range of LPS ports.

- **show port-security pkt-relay filter**
  Displays Learned Port Security (LPS) configuration and table entries.

MIB Objects

- **lpsPacketRelay**
  - **lpsPacketRelaySourceUdpStatus**
  - **lpsPacketRelayDestinationUdpStatus**
**show port-security pkt-relay filter**

Displays the protocol filter configuration for LPS packet relay feature.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```bash
-> show port-security pkt-relay filter
Protocol = udp icmp igmp,
UDP Src-Port = 6754-9876,
UDP Dst-Port = 67-68
```
Learned Port Security Commands

output definitions

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Displays the protocol configured for LPS packet filter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP Src-Port</td>
<td>Displays the UDP source port configured for packet filter.</td>
</tr>
<tr>
<td>UDP Dst-Port</td>
<td>Displays the UDP destination port configured for packet filter.</td>
</tr>
</tbody>
</table>

Release History

Release 8.8R2; command was introduced.

Related Commands

- `show port-security pkt-relay filter` Displays the LPS configuration and table entries for individual LPS ports.

MIB Objects

`learnedPortSecurityTable`

- `lpsMaxMacNum`
- `lpsMaxFilteredMacNum`
- `lpsMaxStaticMacNum`
- `lpsOperStatus`
- `lpsAdminStatus`
show port-security

Displays the Learned Port Security (LPS) configuration and table entries.

show port-security {port [chassis/slot/port][-port2] | slot chassis/slot] | sap {violation | {port | linkagg} sap_id}

Syntax Definitions

chassis The chassis identifier.
slot/port[-port2] The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-8).
slot Enter the slot number for a module to specify that the command should include all ports on that module (for example, 6 specifies all ports on the module found in slot 6 of the switch chassis).
sap_id The SAP ID number identifying the service instance. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 and OmniSwitch 6570M.

Defaults

By default, all ports with an LPS configuration are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Displays ports that have an LPS configuration, even if LPS is disabled on the port.
- Use the port parameter with this command to display the LPS configuration for a specific port or a range of ports.
- Use the slot parameter with this command to display the LPS configuration for all the ports on a specific slot.
- MAC addresses learned on the LPS enabled port that are within the specified MAC address range appear as a separate entries in the LPS table as dynamic MAC type addresses.
- The MAC Type field is blank if an authorized MAC address range is configured for the LPS port.

Examples

-> show port-security port 1/1/20
Learned Port Security Commands

Legend: Mac Address: * = address not valid,
Mac Address: & = duplicate static address,

Port: 1/1/20
Admin-State : ENABLED,
Operation Mode : ENABLED,
Max MAC bridged : 3,
Trap Threshold : 1,
Violation : RESTRICT
Max MAC filtered : 5,
Violating MAC : NULL
Pkt-Relay : ENABLED

<table>
<thead>
<tr>
<th>MAC</th>
<th>VLAN</th>
<th>MAC TYPE</th>
<th>OPERATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:11:22:22:22:21</td>
<td>1</td>
<td>STATIC</td>
<td>bridging</td>
</tr>
<tr>
<td>00:11:22:22:22:22</td>
<td>1</td>
<td>STATIC</td>
<td>bridging</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The module slot number and the physical port number on that module.</td>
</tr>
<tr>
<td>Admin-State</td>
<td>The LPS administrative state for the port (Enabled, Disabled, or Locked). Configured through the port-security command.</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>The LPS operational mode for the port (Enabled, Disabled, Restricted, Shutdown, Discard, Locked, or Filtered-only).</td>
</tr>
<tr>
<td>Max MAC bridged</td>
<td>The maximum number of bridged MAC addresses that are allowed on this port. Configured through the port-security maximum command.</td>
</tr>
<tr>
<td>Trap Threshold</td>
<td>The number of bridged MACs to learn before sending a trap. After this number is reached, a trap is sent out for every MAC learned thereafter. If disabled is displayed in this field, the trap threshold is not in force. Configured through the port-security learn-trap-threshold command.</td>
</tr>
<tr>
<td>Violation</td>
<td>The security violation mode for the port (restrict, shutdown, or discard). Configured through the port-security port violation command.</td>
</tr>
<tr>
<td>Max MAC filtered</td>
<td>The maximum number of filtered MAC addresses that the LPS port can learn. Configured through the port-security port max-filtering command.</td>
</tr>
<tr>
<td>Violating MAC</td>
<td>The MAC Address that caused the violation on this port.</td>
</tr>
<tr>
<td>Pkt-Relay</td>
<td>Displays the packet relay configuration status on the port.</td>
</tr>
<tr>
<td>MAC</td>
<td>The MAC address learned dynamically or configured statically on the LPS port. Static MAC addresses configured through the port-security mac command.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The VLAN to which the LPS port belongs.</td>
</tr>
<tr>
<td>MAC TYPE</td>
<td>Indicates if the MAC address was dynamically learned or statically configured as an authorized MAC address for the port.</td>
</tr>
<tr>
<td>OPERATION</td>
<td>The operational status of the MAC address (bridging or filtering).</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command introduced.
Release 7.2.1.R02: **Admin-State** and **Violating MAC** fields added.
Release 8.4.1: **MAC Address**: * = address not valid and **MAC Address**: & = duplicate static address legend added.
Release 8.8R1: **sap** parameter added.
Release 8.8R2: **Pkt-Relay** field added.

**Related Commands**

- **show port-security learning-window** Displays the amount of time during which source learning can occur on all LPS ports.
- **port-security port pkt-relay** Enables packet relay feature on a single or range of LPS ports.

**MIB Objects**

- **learnedPortSecurityTable**
  - lpsAdminStatus
  - lpsOperStatus
  - lpsMaxMacNum
  - lpsLearnTrapThreshold
  - lpsViolationOption
  - lpsMaxFilteredMacNum
  - lpsLoMacRange
  - lpsHiMacRange
  - lpsViolatingMac
  - lpsRelease

- **learnedPortSecurityAgL2MacAddressTable**
  - lpsAgL2MacAddress
  - lpsAgL2VlanId
  - lpsAgL2MacAddressLearnType
  - lpsPacketRelay
show port-security mac-range

Displays the MAC range configured on the Learned Port Security (LPS) ports.

```
show port-security [port chassis/slot/port[-port2] | sap {port | linkagg} sap_id] mac-range
```

### Syntax Definitions

- `chassis/slot/port[-port2]` The chassis, slot and port number (1/1/1). Use a hyphen to specify a range of ports (1/1/1-8).
- `sap_id` The SAP ID number identifying the service instance. This parameter is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 or OmniSwitch 6570M.

### Defaults

By default, all the LPS ports configured with MAC range are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Specify the chassis, slot, and port to view the MAC range configured for the specific port.

### Examples

```
-> show port-security port 1/1/4 mac-range
Port: 1/1/4:
Low MAC Range                  High MAC Range
--------------------------------+----------------------------------------
00:00:00:00:00:00:00            00:00:00:00:00:00:10
00:00:00:44:00:01               00:00:00:66:ff:ff

-> show port-security mac-range
Port: 1/1/2:
Low MAC Range                  High MAC Range
--------------------------------+----------------------------------------
00:00:00:00:00:00:01            00:00:00:00:00:00:20
00:00:00:00:55:01               00:00:00:00:55:ff
00:00:00:66:00:01               00:00:00:99:ff:ff
Port: 1/1/4:
Low MAC Range                  High MAC Range
--------------------------------+----------------------------------------
00:00:00:00:00:00:00            00:00:00:00:00:00:10
00:00:00:44:00:01               00:00:00:66:ff:ff
```
Learned Port Security Commands

show port-security mac-range

output definitions

<table>
<thead>
<tr>
<th>Port</th>
<th>The chassis slot number and the physical port number on that chassis.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low MAC Range</td>
<td>MAC address that defines the lower end of a MAC address range. Configured through the <code>port-security mac-range</code> command.</td>
</tr>
<tr>
<td>High MAC Range</td>
<td>MAC address that defines the higher end of a MAC address range. Configured through the <code>port-security mac-range</code> command.</td>
</tr>
</tbody>
</table>

Release History

Release 8.5R3; command introduced.
Release 8.8R1; sap parameter added.

Related Commands

port-security mac-range Configures a list of authorized MAC addresses by defining a range of addresses allowed on the port.

MIB Objects

learnedPortSecurityL2MacRangeTable
   lpsL2LowMacAddress
   lpsL2HighMacAddress
show port-security brief

Displays the LPS port configuration for all the LPS ports.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The LPS port parameter values are displayed even if the LPS is disabled on the port.
- The operation mode displayed for the LPS port is based on a combination of the existing administrative status and the operational status of the port, the result of which is one of the following values:
  - Enabled
  - Restricted (only when the administrative status is enabled)
  - Shutdown (only when the administrative status is enabled)
  - Discard (only when the administrative status is enabled)
  - Disabled
  - Locked
  - Filtered_only

Examples

-> show port-security brief

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>Operation Mode</th>
<th>Max Bridge</th>
<th>Max Filter</th>
<th>Nb Dyn Br</th>
<th>Nb Dyn Fltr</th>
<th>Nb Static Br</th>
<th>Nb Static Fltr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>ENABLED</td>
<td>5</td>
<td>100</td>
<td>5</td>
<td>10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/2</td>
<td>ENABLED</td>
<td>5</td>
<td>100</td>
<td>0</td>
<td>10</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>1/3</td>
<td>RESTRICTED</td>
<td>5</td>
<td>100</td>
<td>5</td>
<td>100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1/4</td>
<td>SHUTDOWN</td>
<td>5</td>
<td>100</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>1/5</td>
<td>DISABLED</td>
<td>5</td>
<td>100</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>1/6</td>
<td>LOCKED</td>
<td>5</td>
<td>100</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
**output definitions**

<table>
<thead>
<tr>
<th>Slot/Port</th>
<th>The slot number for the module and the physical port number on that module (e.g., 1/2 specifies port 2 on slot 1).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation Mode</td>
<td>Displays the status of the LPS port.</td>
</tr>
<tr>
<td>Max Bridge</td>
<td>The maximum number of bridged MAC addresses that are allowed on the LPS port. Configured through the <code>port-security maximum</code> command.</td>
</tr>
<tr>
<td>Max Filter</td>
<td>The maximum number of filtered MAC addresses that the LPS port can learn. Configured through the <code>port-security port max-filtering</code> command.</td>
</tr>
<tr>
<td>Nb Macs Dyn Br</td>
<td>Total number of bridged MAC addresses learned on the LPS port.</td>
</tr>
<tr>
<td>Nb Macs Dyn Fltr</td>
<td>Total number of filtered MAC addresses learned on the LPS port.</td>
</tr>
<tr>
<td>Nb Macs Static Br</td>
<td>Total number of bridged static MAC addresses (configured static and MAC addresses learned as pseudo-static) on the LPS port.</td>
</tr>
<tr>
<td>Nb Macs Static Fltr</td>
<td>Total number of filtered static MAC addresses configured on the LPS port.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.2.1.R02; command was introduced.

**Related Commands**

`show port-security pkt-relay filter` Displays the LPS configuration and table entries for individual LPS ports.

**MIB Objects**

`learnedPortSecurityTable`
- `lpsMaxMacNum`
- `lpsMaxFilteredMacNum`
- `lpsMaxStaticMacNum`
- `lpsOperStatus`
- `lpsAdminStatus`
**show port-security learning-window**

Displays the source learning window configuration.

```
show port-security learning-window
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The source learning time limit is a switch-wide parameter that applies to all ports that have LPS enabled.
- If the learning window time is not set, then no source learning time limit is applied to LPS ports.
- Even after the LPS learning window time expires, dynamic MAC addresses are learned as filtered addresses until the maximum number of filtered MAC addresses allowed for the LPS port is reached. For example, if the maximum number of bridged MAC addresses allowed is set to 30 and the learning window expires when the port has only learned 15, the port is still allowed to learn an additional 15 filtered MAC addresses.

### Examples

```
-> show port-security learning-window
Learning-Window       = 2 min,
Convert-to-static     = DISABLE,
No Aging              = DISABLE,
Boot Up               = ENABLE,
Remaining Learning Window = 120 sec
Learn As Static       = ENABLE,
Mac Move              = DISABLE,
```
Learned Port Security Commands

**show port-security learning-window**

<table>
<thead>
<tr>
<th>output definitions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Learning-Window</strong></td>
<td>The configured amount of time during which the LPS port can learn new MAC addresses. This value of this field is set to <strong>INFINITY</strong> when the learning time window is set to zero (no source learning time restriction on LPS ports).</td>
</tr>
<tr>
<td><strong>Convert-to-static</strong></td>
<td>Indicates whether or not dynamic bridged or pseudo-static MACs are converted to static MACs (<strong>ENABLED</strong> or <strong>DISABLED</strong>). This option is always disabled when the LPS learning window is set to infinity (zero).</td>
</tr>
<tr>
<td><strong>No Aging</strong></td>
<td>Indicates whether or not bridged MAC addresses are learned as pseudo-static MAC addresses, which do not age out during the LPS learning window time period (<strong>DISABLED</strong> or <strong>ENABLED</strong>).</td>
</tr>
<tr>
<td><strong>Boot Up</strong></td>
<td>Indicates whether or not the LPS learning window automatically starts when the switch boots up (<strong>enabled</strong> or <strong>disabled</strong>).</td>
</tr>
<tr>
<td><strong>Learn As Static</strong></td>
<td>Indicates whether or not dynamic MAC addresses are automatically learned as static MAC addresses during the LPS learning window time period. The <strong>Learn As Static</strong> and <strong>No Aging</strong> learning window options are mutually exclusive.</td>
</tr>
<tr>
<td><strong>Mac Move</strong></td>
<td>Indicates whether or not pseudo-static MAC addresses are allowed to move to a different port in the same VLAN during the LPS learning window time period. The <strong>Mac Move</strong> learning window option applies only when the <strong>No Aging</strong> option is enabled.</td>
</tr>
<tr>
<td><strong>Remaining Learning Window</strong></td>
<td>The remaining amount of time during which the LPS port can learn MAC addresses. If the learning time window is set to <strong>INFINITY</strong> (zero), this field does not display in the show command output.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.
Release 7.2.1.R02; **LPS Shutdown Config** field changed to **Learning-Window**, **No Aging** and **Boot Up** fields added.
Release 8.2.1; **Learn As Static** and **Mac Move** fields added.

**Related Commands**

- `port-security learning-window` Configures the learning window parameters that are applied to all LPS ports.
- `show port-security pkt-relay filter` Displays the LPS configuration and table entries for individual LPS ports.

**MIB Objects**

- `learnedPortSecurityGlobalGroup`
  - `lpsLearningWindowTime`
  - `lpsLearningWindowTimeWithStaticConversion`
  - `lpsLearningWindowNoAging`
  - `lpsLearningWindowBootupStatus`
  - `lpsLearningWindowLearnAsStatic`,
  - `lpsLearningWindowPseudoMacMove`
  - `lpsLearningWindowTimeRemaining`
48  Port Mirroring and Monitoring Commands

The Port Mirroring and Port Monitoring features are primarily used as diagnostic tools.

The Port Mirroring feature allows you to have all the inbound and outbound traffic of an Ethernet port sent to another port on the switch. When you enable port mirroring, the active, or “mirrored,” port transmits and receives network traffic normally and the “mirroring” port receives a copy of all transmit and receive traffic to the active port. You can connect an RMON probe or network analysis device to the mirroring port to see an exact duplication of traffic on the mirrored port without disrupting network traffic to and from the mirrored port.

The Port Monitoring feature allows you to capture and examine the data traffic to and from a monitored Ethernet port.

MIB information for the Port Mirroring commands is as follows:

   Filename:   ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB.mib
   Module:     alcatelIND1PortMirrorMonitoringMIB

The following table summarizes the available commands:

| Port Mirroring Commands                  | port-mirroring source destination |
|                                        | port-mirroring                      |
|                                        | port-mirroring traffic-priority     |
|                                        | show port-mirroring status          |

| Port Monitoring Commands                | port-monitoring source             |
|                                       | port-monitoring                    |
|                                       | show port-monitoring status        |
|                                       | show port-monitoring file          |
**port-mirroring source destination**

Defines the port to mirror and the port that is to receive data from the mirrored port. Also, enables or disables remote port mirroring.

```
port-mirroring port_mirror_sessionid source {port chassis/slot/port[-port2]} destination {port chassis/slot/port[-port2] | linkagg linkagg[-linkagg2]} [rpmir-vlan vlan_id] [bidirectional | inport | outport] [loopback] [unblocked-vlan vlan_id] [tag-remove] [enable | disable]
```

```
port-mirroring port_mirror_sessionid no source {port chassis/slot/port[-port2] [chassis/slot/port[-port2]...]
```

```
port-mirroring port_mirror_sessionid no destination {port chassis/slot/port[-port2] [chassis/slot/port[-port2]...]} [linkagg linkagg[-linkagg2] [linkagg[-linkagg2]...]
```

### Syntax Definitions

- **port_mirror_sessionid**: Mirroring session identifier.
- **source**: Specifies source port, or range of ports desired to be mirrored.
- **destination**: Specifies the destination port or linkagg that receives all the mirrored packets.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number. Use a hyphen to specify a range of ports.
- **linkagg[-linkagg2]**: The destination link aggregate. Use a hyphen to specify a range. *This parameter is not supported on OS6360, OS6465, OS6560 and OS6570M.*
- **rpmir-vlan vlan_id**: Specifies a reserved VLAN to carry the mirroring traffic. Use this parameter to configure remote port mirroring. See “Usage Guidelines - Remote Port Mirroring” below for more information.
- **bidirectional**: Specifies bidirectional port mirroring.
- **inport**: Specifies incoming unidirectional port mirroring.
- **outport**: Specifies outgoing unidirectional port mirroring.
- **loopback**: Enables or disables loopback mechanism on the destination port for the session. *This parameter is supported only on the OmniSwitch 6465.*
- **unblocked-vlan vlan_id**: Specifies the VLAN that is to be protected from Spanning Tree changes when port mirroring is active. Ports in this VLAN remain unblocked.
- **tag-remove**: Removes the VLAN tag on mirrored traffic that egresses out of the destination mirroring ports. *This parameter is supported only on the OmniSwitch 9900.*
- **enable**: Enables port mirroring status.
- **disable**: Disables port mirroring status.
Port Mirroring and Monitoring Commands

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bidirectional</td>
<td>bidirectional</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Port mirroring cannot be configured on an AppMon enabled port.
- You can configure a port mirroring and a port monitoring session on the same network interface module.
- A mirroring port cannot be assigned to a tagged VLAN port.
- When a port is configured as a mirroring port, it does not belong to any VLAN. Inbound traffic to the mirroring port is dropped since it does not belong to any VLAN.
- To mirror traffic from SAP port to destination port, explicitly create a VLAN same as the SAP VLAN.
- Spanning tree is disabled by default on a mirroring port.
- Port mirroring is not supported on logical link aggregate ports. However, it is supported on individual ports that are members of a link aggregate.
- Port mirroring destination port can be a link aggregate. This functionality is not supported on OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 and OmniSwitch 6570M.
- Use the `port mirroring source destination` command to define the mirrored port and enable port mirroring status. Use the `port mirroring` command to enable the port mirroring session.
- Specify the `vlan_id` number of the mirroring port that is to remain unblocked when the command is executed. The unblocked VLAN becomes the default VLAN for the mirroring port. This VLAN handles the inbound traffic for the mirroring port. Spanning Tree remains disabled on the unblocked VLAN.
- A maximum of 128 source mirroring ports can be configured. In case of mirroring to LACP Link Aggregate, only the first 8 aggregable ports will be used for mirroring.
- Unblocked VLAN and RPMIR configuration cannot co-exist in the same port mirroring session.
- A port/link aggregate which is to be configured as a mirroring destination should have no prior configuration on it, for example, a MVRP enabled port/link aggregate cannot be configured as a mirroring destination. The only exception to this rule is that a port can be a untagged or a tagged member of a standard VLAN.
Port Mirroring and Monitoring Commands

- Any protocol/feature configurations on existing mirroring destinations would fail. All such configuration attempts would result in an error. The only exception to this is that if a mirroring destination is part of a mirroring session which has remote port mirroring VLAN configured (RPMIR VLAN) then such a destination can be made a tagged and/or untagged member of standard VLAN(s).

- A maximum of one mirroring session with two mirroring destinations or a maximum of two sessions each having a single mirroring destination is supported on OmniSwitch 6860, OmniSwitch 6860N, OmniSwitch 6865, and OmniSwitch 6900.

- Supports single destination mirroring port per session and seven port mirroring sessions in a system on OmniSwitch 6465, OmniSwitch 6560 and OmniSwitch 6570M platforms.

- Supports multiple destination mirroring port and link aggregates per session and seven port mirroring sessions, and 128 destination mirroring ports or link aggregates in a system. This functionality is supported on OmniSwitch 9900.

- Supports policy based multiple destination mirroring on a single port mirroring session. This functionality is supported on OmniSwitch 9900.
  - To enable this functionality, configure port mirroring session with destination port and then apply policy based configuration on the port mirroring session.
  - Use the QoS mirror session attribute to support policy based multiple destination mirroring. QoS mirroring session attribute can be specified as a part of policy action in the policy action command. Mirroring can be done on the ingress packets only. Only one session ID is supported for policy based mirroring, thus all the policies must specify the same session ID. For more information on policy based mirroring, see Chapter 37, “QoS Policy Commands.”

- Use the tag remove option to remove the VLAN tag on mirrored traffic that egresses out of destination mirroring ports. For double tagged mirrored packet, this option removes the outer VLAN tag.

- RPMIR and tag remove configuration is mutually exclusive and hence cannot co-exist in the same port mirroring session.

Usage Guidelines - Remote Port Mirroring

- Use the rpmir-vlan parameter and VLAN ID with this command to configure remote port mirroring and to assign the VLAN ID for remote port mirroring.
  - Remote port mirroring over a link aggregate is not supported on the OmniSwitch 6360, OmniSwitch 6465, OmniSwitch 6560 and OmniSwitch 6570M.
  - Remote port mirroring in loopback mode is supported only on OmniSwitch 6465.

- The VLAN ID assigned for remote port mirroring cannot be assigned to a general port mirroring port.

- There must not be any physical loop present in the remote port mirroring VLAN.

- Source learning must be disabled or overridden on the ports belonging to the remote port mirroring VLAN on intermediate and destination switches.

- The QoS redirect feature can be used to override source learning.

- The mac-learning command can also be used to disable learning on the RPMIR VLAN ID.

- VLAN 1 cannot be configured as the RPMIR VLAN.

- When mirroring configuration is removed from a mirroring destination, the port/link aggregate is made an untagged member of VLAN 1. The only exception to this is when the destination in a mirroring session with RPMIR configuration.
Port Mirroring and Monitoring Commands

- When RPMIR-loopback session is enabled, source learning on the loopback port is disabled.
- When RPMIR-loopback session is enabled, STP for the configured RPMIR-VLAN alone is disabled.
- To revert the RPMIR session from loopback to default the entire session must be removed and configured again.

Examples

-> port-mirroring 6 source port 1/2/2 destination port 1/1/3
-> port-mirroring 6 destination port 1/1/3 rpmir-vlan 7
-> port-mirroring 6 no source port 1/2/2

-> port-mirroring 7 source port 1/2/3 destination linkagg 3 unblocked-vlan 750
-> port-mirroring 7 source port 1/2/3 outport

-> port-mirroring 7 source port 1/2/3 destination linkagg 3 tag-remove

-> port-mirroring 9 source port 1/1/23 destination port 1/1/24
-> port-mirroring 9 disable

-> port mirroring 1 source port 1/1/1 destination port 1/1/3 bidirectional rpmir-vlan 100 loopback enable
-> port mirroring 1 source port 1/1/1 destination port 1/1/3 bidirectional rpmir-vlan 100 loopback disable

Release History

Release 7.1.1; command introduced.
Release 8.4.1.R03; Mirroring to a link aggregate supported on OmniSwitch 6900 and OmniSwitch 6860.
Release 8.6.R1; **tag-remove** keyword added, policy based multiple destination mirroring supported on OmniSwitch 9900.
Release 8.7 R2; **loopback** keyword added, RPMIR Loopback Session supported on OmniSwitch 6465.

Related Commands

**port-mirroring**
Enables, disables, or deletes a port mirroring session.

**show port-mirroring status**
Displays the status of mirrored ports. This value may be enabled or disabled.

MIB Objects

mirrorTable
- mirrorMirroringIfindex
- mirrorDirection
- mirrorStatus
- mirrorUnblockedVLAN
- mirrorRowStatus
- mirrorDirection
- mirrorModeLoopback
- mirrorSessOperStatus
- mirrorTaggedVLAN
- mirrorDstTagRemove
**port-mirroring**

Enables, disables, or deletes a port mirroring session.

```
port-mirroring port_mirror_sessionid {enable | disable}
no port-mirroring port_mirror_sessionid
```

### Syntax Definitions

- **port_mirror_sessionid**  
  Mirroring session identifier.
- **enable**  
  Enables port mirroring.
- **disable**  
  Disables port mirroring.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of this command to delete a port mirroring session.
- Use the **port-mirroring source destination** command to specify the mirrored ports and destination port before using this command to enable or disable port mirroring activity for the particular port mirroring session.

### Examples

```
-> port-mirroring 6 enable
-> port-mirroring 6 disable
-> no port-mirroring 6
```

### Release History

Release 7.1.1; command introduced.
Related Commands

port-mirroring source
destination

show port-mirroring status

Defines a port to mirror and the port that is to receive data from the mirrored port, and enables or disables port mirroring status.

Displays the status of mirrored ports. This value may be enabled or disabled.

MIB Objects

mirrorTable

mirrorMirroringIfindex
mirrorTaggedVLAN
mirrorStatus
port-mirroring traffic-priority

This command enables to set the priority for mirroring traffic.

port-mirroring traffic-priority {normal | high}

Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>Sets the priority for mirroring traffic to normal.</td>
</tr>
<tr>
<td>high</td>
<td>Sets the priority for mirroring traffic to high.</td>
</tr>
</tbody>
</table>

Defaults

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

When the traffic priority is set to high, ingress and egress mirroring receive strict priority over other clients (regular received, not mirrored, traffic, and so on).

Examples

-> port-mirroring traffic-priority normal
-> port-mirroring traffic-priority high

Release History

Release 8.7R3; command introduced.

Related Commands

show port-mirroring status Displays the status of mirrored ports. This value may be enabled or disabled.

MIB Objects

mirrorTrafficPriority
**port-monitoring source**

Configures a port monitoring session.

```
port-monitoring port_monitor_sessionid source port chassis/slot/port[-port2] [file filename [size filesize] | no file | overwrite {on | off}] [inport | outport | bidirectional] [timeout seconds] [enable | disable] [capture-type {full | brief}]
```

```
port-monitoring port_monitor_sessionid no source port chassis/slot/port[-port2]
```

### Syntax Definitions

- **port_monitor_sessionid**: Monitoring session identifier.
- **chassis**: The chassis identifier.
- **slot/port[-port2]**: The slot and port number. Use a hyphen to specify a range of ports.
- **filename**: Specifies a file name and pathname for capturing information related to the monitoring session (for example, `/flash/port2.enc`).
- **filesize**: Specifies the size of the file in 64K byte increments. For example, a value of 3 would specify a size of (3 x 64K) bytes.
- **no file**: *This option is not supported at this time.*
- **on**: Specifies that capturing of data packets into the port monitoring file continues and old information is overwritten if the total data exceeds the specified file size.
- **off**: Specifies that capturing of data packets into the port monitoring file is stopped when the maximum file size is reached.
- **inport**: Specifies incoming unidirectional port monitoring.
- **outport**: Specifies outgoing unidirectional port monitoring.
- **seconds**: Specifies the number of seconds after which the session is disabled.
- **enable**: Enables the port monitoring status.
- **disable**: Disables the port monitoring status.
- **full**: Captures port monitoring information in detail.
- **brief**: Captures only the concise port monitoring data transmitted.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>filesize</td>
<td>1</td>
</tr>
<tr>
<td>on/off</td>
<td>on</td>
</tr>
<tr>
<td>bidirectional</td>
<td>inport</td>
</tr>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>capture-type</td>
<td>brief</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Port monitoring cannot be configured on an AppMon enabled port.
- If the `ip interface 'no forward'` parameter is configured in conjunction with port-monitoring on a port which is being used for switch IP connectivity, IP connectivity may be lost. Either port-monitoring or 'no forward' must be disabled to allow IP connectivity.
- You can configure a port mirroring and a port monitoring session on the same NI.
- If the port monitoring capture-type is set to `brief`, the first 64 bytes of the traffic is captured. If the port-monitoring capture-type is set to `full`, the entire packet is captured.
- By default, a file called `pmonitor.enc` is created in the `/flash` directory when you configure and enable a port monitoring session. Use the `file` option to create a user-specified file.
- The `/flash` directory is the default and the only directory used to capture the port monitoring files.
- The format of the file created is compliant with the ENC file format (Network General Sniffer Network Analyzer Format).
- By default, the recent frames overwrite the older frames in a port monitoring file if the total data exceeds the specified file size. Use the `overwrite off` option to prevent this from occurring.

Examples

- `-> port-monitoring 6 source port 1/2/3`
- `-> port-monitoring 6 source port 1/2/3 file /flash/user_port size 2 enable`
- `-> port-monitoring 6 source port 1/2/3 file /flash/user_port capture-type full`
- `-> port-monitoring 10 source port 1/4/22-30`
- `-> port-monitoring 10 no source port 1/4/30`

Release History

Release 7.1.1; command introduced.
Port Mirroring and Monitoring Commands

Related Commands

port-monitoring
   Disables, pauses, resumes, or deletes a port monitoring session.
show port-monitoring status
   Displays the port monitoring status.
show port-monitoring file
   Displays the port monitoring data.

MIB Objects

monitorTable
   monitor
   monitorSessionNumber
   monitorIfindex
   monitorFileStatus
   monitorFileName
   monitorFileSize
   monitorScreenStatus
   monitorScreenLine
   monitorCaptureType
   monitorTrafficType
   monitorStatus
   monitorFileOverWrite
   monitorDirection
   monitorTimeout
**port-monitoring**

Disables, pauses, resume, or deletes an existing port monitoring session.

`port-monitoring port_monitor_sessionid {disable | pause | resume}`

`no port-monitoring port_monitor_sessionid`

---

**Syntax Definitions**

- `port_monitor_sessionid`: Monitoring session identifier.
- `disable`: Disables the port monitoring session.
- `pause`: Pauses the port monitoring session.
- `resume`: Resumes the port monitoring session.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use the **no** form of this command to delete a port monitoring session.

**Examples**

- `-> port-monitoring 6 pause`
- `-> port-monitoring 6 disable`
- `-> port-monitoring 6 resume`
- `-> no port-monitoring 6`

---

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **port-monitoring** Configures a port monitoring session.
- **show port-monitoring status** Displays the port monitoring status.

MIB Objects

- **monitorTable**
  - **monitorSessionNumber**
  - **monitorScreenStatus**
**show port-mirroring status**

Displays the status of mirrored ports.

`show port-mirroring status [port_mirror_sessionid]`

**Syntax Definitions**

`port_mirror_sessionid` Mirroring session identifier.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platforms Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
</tr>
<tr>
<td>6465</td>
</tr>
<tr>
<td>6560</td>
</tr>
<tr>
<td>6570M</td>
</tr>
<tr>
<td>6860</td>
</tr>
<tr>
<td>6860N</td>
</tr>
<tr>
<td>6865</td>
</tr>
<tr>
<td>6900</td>
</tr>
<tr>
<td>6900V72/C32</td>
</tr>
<tr>
<td>6900X48C6/T48C6</td>
</tr>
<tr>
<td>6900X48C4E/V48C8/C32</td>
</tr>
<tr>
<td>6900T24C2/X24C2</td>
</tr>
<tr>
<td>9900</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8/C32</th>
<th>6900T24C2/X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If a port mirroring session identifier is not specified with this command, then all port mirroring sessions are displayed.

**Examples**

```
-> show port-mirroring status
Session    Mirror        Mirror      Unblocked   RPMIR            Config   Oper
Destination    Direction     Vlan       Vlan     Mode   Status   Status
----------+-----------+----------------+--------+---------+-------+-------+--------
1.     1/1/11       bidirectional  NONE      100     loopback Enable    on
----------+-----------+----------------+--------+---------+-------+------+--------
Mirror      Source
----------+-----------+--------------+----------+---------+----------+--------
1.      1/1/2       bidirectional     -         -      Enable    On
1.      1/1/3       bidirectional     -         -      Enable    On
1.      1/1/4       bidirectional     -         -      Enable    On
1.      1/1/5       bidirectional     -         -      Enable    On
```

**output definitions**

- **Session** The port mirroring session identifier.
- **Mirror Destination** The location of the mirrored port.
- **Mirror Direction** The direction of the mirroring or mirrored port, which can be **bidirectional** (the default), **inport**, or **outport**.
- **Unblocked VLAN** The mirroring VLAN ID number.
**output definitions (continued)**

| **RPMIR VLAN** | The reserved VLAN to carry the mirroring traffic. |
| **Mode** | Displays if the Loopback mode is configured for RPMIR session. |
| **Config Status** | The configuration status of the session. |
| **Oper Status** | The current status of the mirroring or mirrored port. |
| **Mirror Source** | The location of the mirroring port. |

**Release History**

Release 7.1.1; command introduced.
Release 8.7 R2; **Mode** output added, RPMIR Loopback Session is supported on OmniSwitch 6465.

**Related Commands**

- **port-mirroring**
  Enables, disables, or deletes a port mirroring session.
- **port-mirroring source destination**
  Defines a port to mirror and a port that receives data from the mirrored port, and enables or disables port mirroring status.

**MIB Objects**

- mirrorTable
  - mirrorMirroringIfindex
  - mirrorMirroredIfindex
  - mirrorDirection
  - mirrorStatus
  - mirrorSessionNumber
  - mirrorSessOperStatus
  - mirrorSrcStatus
  - mirrorModeLoopback
  - mirrorSrcDirection
  - mirrorSrcRowStatus
  - mirrorSrcOperStatus
  - mirrorUnblockedVLAN
show port-monitoring status

Displays port monitoring status.

```
show port-monitoring status [port_monitor_sessionid]
```

**Syntax Definitions**

| `port_monitor_sessionid` | Monitoring session identifier. |

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If a port monitoring session identifier is not specified with this command, then all port monitoring sessions are displayed.

**Examples**

```shell
-> show port-monitoring status

Src Dir write Stat Stat Type Size Name
----------+------+----------+--------+---------+--------+-------+--------------------------
1. 1/1/2 Out OFF OFF OFF Brief 64K /flash/pm.enc
```

**output definitions**

<table>
<thead>
<tr>
<th>Sess</th>
<th>Session - The port monitoring session identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mon. Src</td>
<td>Monitor Source - The source ports that are monitored.</td>
</tr>
<tr>
<td>Mon Dir</td>
<td>Monitor Direction - The direction of the monitoring session, which can be bidirectional (the default), inport, or outport.</td>
</tr>
<tr>
<td>Overwrite</td>
<td>Whether files created by a port monitoring session can be overwritten. The default is ON.</td>
</tr>
<tr>
<td>Oper Stat</td>
<td>Operating Status - The current operating status of the port monitoring session (on/off).</td>
</tr>
</tbody>
</table>
Port Mirroring and Monitoring Commands

show port-monitoring status

output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Stat</td>
<td>Admin Status - The current administrative status of the port monitoring session (on/off).</td>
</tr>
<tr>
<td>Capt Type</td>
<td>Capture type:</td>
</tr>
<tr>
<td></td>
<td>Brief - captures only 64 bytes of data per traffic data packet.</td>
</tr>
<tr>
<td></td>
<td>Full - captures the entire packet.</td>
</tr>
<tr>
<td>Max Size</td>
<td>Maximum Size - The maximum size of the port monitoring file.</td>
</tr>
<tr>
<td>File Name</td>
<td>The name of the port monitoring file.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

- **port-monitoring source** Configures a port monitoring session.
- **port-monitoring** Disables, pauses, resumes, or deletes a port monitoring session.
- **show port-monitoring file** Displays port monitoring data.

MIB Objects

- monitorTable
  - monitorSessionNumber
  - monitorIfindex
  - monitorStatus
  - monitorFileStatus
  - monitorFileName
  - monitorFileSize
  - monitorScreenStatus
  - monitorScreenLine
  - monitorTrafficType
  - monitorDirection
  - monitorTimeout
  - monitorCaptureType
  - monitorFileOverWrite
  - monitorDirection
**show port-monitoring file**

Displays port monitoring data.

**show port-monitoring file** *port_monitor_sessionid*

### Syntax Definitions

**port_monitor_sessionid**

Monitoring session identifier.

### Defaults

A single line from the captured packet is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Only a single line from the captured packet is displayed, even though the full packet is captured. To view the entire packet, download the file and view it using a compatible network analyzer tool.

### Examples

```plaintext
-> show port-monitoring file 1
```

### output definitions

- **Destination**: The destination MAC address of the packet.
- **Source**: The source MAC address of the packet.
- **Type**: The type of packet.
- **Data**: The packet displayed in hexadecimal format.
**Release History**
Release 7.1.1; command introduced.

**Related Commands**

- **port-monitoring source** Configures a port monitoring session.
- **port-monitoring** Disables, pauses, resumes, or deletes a port monitoring session.
- **show port-monitoring status** Displays the port monitoring status.

**MIB Objects**

- `monitorTable`
  - `monitorSessionNumber`
  - `monitorIfindex`
  - `monitorTrafficType`
  - `monitorFileStatus`
  - `monitorFileName`
  - `monitorFileSize`
  - `monitorScreenStatus`
  - `monitorScreenLine`
sFlow is a network monitoring technology that gives visibility into the activity of the network, by providing network usage information. It provides the data required to effectively control and manage the network usage. sFlow is a sampling technology that meets the requirements for a network traffic monitoring solution.

sFlow provides a network-wide view of usage and active routes. It is used for measuring network traffic, collecting, storing, and analyzing the traffic data. As it is scalable, that doesn’t add significant network load. sFlow is an industry standard with many vendors delivering products with this support. Some of the applications of the sFlow data include:

- Detecting, diagnosing, and fixing network problems
- Real-time congestion management
- Detecting unauthorized network activity
- Usage accounting and billing
- Understanding application mix
- Route profiling and peer optimization
- Capacity planning

sFlow is a sampling technology embedded within switches/routers. It provides the ability to monitor the traffic flows. It requires an sFlow agent software process running as part of the switch software and a sFlow collector which receives and analyses the monitored data. The sFlow collector makes use of SNMP to communicate with an sFlow agent in order to configure sFlow monitoring on the device (switch).

An sFlow agent running on the switch/router combines interface counters and traffic flow (packet) samples, preferably, on all the interfaces into sFlow datagrams that are sent across the network to an sFlow collector.

Packet sampling on the switch/router is typically performed by the switching/routing ASICs, providing wire-speed performance. In this case, an sFlow agent does very little processing, by packaging data into sFlow datagrams that are immediately sent on network. This minimizes the memory and CPU utilization by the sFlow agent.

MIB information for the sFlow commands is as follows:

- **Filename:** ALCATEL-IND1-PORT-MIRRORING-MONITORING-MIB.mib
  **Module:** alcatelIND1PortMirrorMonitoringMIB

- **Filename:** SFLOW-MIB.MIB.mib
  **Module:** sFlow
A summary of the available commands is listed here:

- sflow agent
- sflow receiver
- sflow sampler
- sflow poller
- show sflow agent
- show sflow receiver
- show sflow sampler
- show sflow poller
**sflow agent**

Configures a specific sFlow agent IP address.

`sflow agent ip ip_address`

`no sflow agent ip ip_address`

---

**Syntax Definitions**

`ip_address` The sFlow agent IP address.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td><code>0.0.0.0</code></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete the IP address.
- If no IP address is configured, 0.0.0.0 is used.
- If no IP address is configured but the Loopback0 address is configured, the Loopback0 address is used.

**Examples**

- `-> sflow agent ip 192.168.1.1`
- `-> no sflow agent ip 192.168.1.1`

**Release History**

Release 7.1.1; command was introduced.
Release 7.3.4; command deprecated. Use `ip service source-ip`. 
Related Commands

**show sflow agent** Displays the agent table.

MIB Objects

```
mironSFlowObjects
   alasFlowAgentConfigType
   alasFlowAgentAddressType
   alasFlowAgentAddress
```
sflow receiver

Sets the destination hosts where the sFlow datagrams are sent out. If there are multiple destinations, then each destination has an instance of the receiver. All these receivers are attached to the sFlow manager instance and to an associated sampler/poller.

```
vrf {name} sflow receiver receiver_index {name string | timeout {seconds | forever} | address {ip_address | ipv6_address | domain_name} | udp-port port | packet-size size version num | release}
```

## Syntax Definitions

- **name**: The name of the VRF to be configured for the sflow receiver.
- **receiver_index**: The receiver index number.
- **string**: The name.
- **seconds | forever**: Specifies the timeout value.
- **ip_address**: Specifies the 32-bit IPv4 address.
- **ipv6_address**: Specifies the 128-bit IPv6 address.
- **domain_name**: Specifies a Fully Qualified Domain Name (FQDN). The domain name can be up to 255 characters in length.
- **port**: Specifies the UDP (destination) port.
- **size**: Specifies the maximum number of data bytes (size) that can be sent.
- **num**: Specifies the version number.

## Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>empty</td>
</tr>
<tr>
<td>seconds</td>
<td>0</td>
</tr>
<tr>
<td>ip_address</td>
<td>0.0.0.0(ipv4)</td>
</tr>
<tr>
<td>port</td>
<td>6343</td>
</tr>
<tr>
<td>size</td>
<td>1400</td>
</tr>
<tr>
<td>version num</td>
<td>5</td>
</tr>
</tbody>
</table>

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Use the `release` parameter at the end of the command to delete a receiver.

- Use the `domain_name` option to specify an FQDN instead of an IPv4 or IPv6 address. The switch will then resolve the domain name to an IP address. Make sure the specified domain name maps to a valid and reachable address. If the address is not valid or cannot be reached, then flow and counter samples may not be sent out of the sFlow agent as expected.

- After the IPv4 or IPv6 address for the specified domain name is determined, a refresh is triggered every 30 seconds. If the mapping of the domain name to an IP address changes before the next refresh, both flow and counter samples are not sent to the new address until the next refresh occurs.

- If the VRF is not configured then the default VRF is applied.

Examples

- `sflow receiver 1 name Golden Rcvr1 address 198.206.181.3`
- `vrf ipvxlan sflow receiver 1 name Golden Rcvr1 address 198.206.181.3`
- `sflow receiver 1 name Golden Rcvr1 address upam.omnivista.com`
- `sflow receiver 1 release`

Release History

Release 7.1.1; command was introduced.
Release 8.5R1; `domain_name` parameter option added.
Release 8.9R1; `vrf` parameter introduced.

Related Commands

`show sflow receiver` Displays the receiver table.

MIB Objects

`sFlowRcvrTable`

- `sFlowRcvrIndex`
- `sFlowRcvrOwner`
- `sFlowRcvrTimeout`
- `sFlowRcvrMaximumDatagramSize`
- `sFlowRcvrAddressType`
- `sFlowRcvrAddress`
- `sFlowRcvrPort`
- `sFlowRcvrDatagramVersion`
**sflow sampler**

Gets the hardware sampled from Q-dispatcher and fills up the sampler part of the UDP datagram.

```
<vrf {name} sflow sampler num port chassis/slot/port[-port] {receiver receiver_index | rate value | sample-hdr-size size}>
```

```
o sflow sampler num port [chassis_id/slot/port[-port]]
```

**Syntax Definitions**

- **name**: The name of the VRF to be configured for the sflow sampler.
- **num**: Specifies the instance ID.
- **chassis**: The chassis identifier.
- **slot/port[-port]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
- **receiver_index**: Specifies the receiver index.
- **value**: Specifies the rate value for packet sampling.
- **size**: Specifies the maximum number of bytes (size) that can be copied from a sampled packet.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>receiver_index</td>
<td>0</td>
</tr>
<tr>
<td>value</td>
<td>0</td>
</tr>
<tr>
<td>size</td>
<td>128</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<p>| | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>6465</td>
<td>6560</td>
<td>6570M</td>
<td>6860</td>
<td>6860N</td>
<td>6865</td>
<td>6900</td>
<td>6900</td>
<td>6900</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to delete a sampler.
- A sampling rate of 1 counts all packets. A sampling rate of 0 disables sampling.
- If the VRF is not configured then the default VRF is applied.
Examples

-> sflow sampler 1 port 1/2/1 receiver 1 rate 5 sample-hdr-size 64
-> vrf ipvlan sflow sampler 1 port 1/2/1 receiver 1 rate 5 sample-hdr-size 64
-> no sflow sampler 1 port 1/2/1-5

Release History

Release 7.1.1; command was introduced.
Release 8.9R1; vrf parameter introduced.

Related Commands

show sflow sampler

Displays the sampler table.

MIB Objects

sFlowFsTable
  sFlowFsDataSource
  sFlowFsInstance
  sFlowFsReceiver
  sFlowFsPacketSamplingRate
  sFlowFsMaximumHeaderSize
sflow poller

Gets counter samples from ethernet driver and fills up the counter part of the UDP datagram.

```
configuration>
  vrf {name} sflow poller num port chassis/slot/port[-port] [receiver receiver_index | interval value]
no sflow poller num port [chassis_id/slot/port[-port]]
```

### Syntax Definitions

- **name**: The name of the VRF to be configured for the sflow poller.
- **num**: Specifies the instance ID.
- **chassis**: The chassis identifier.
- **slot/port[-port]**: The slot and port number (3/1). Use a hyphen to specify a range of ports (3/1-5).
- **receiver_index**: Specifies the receiver index.
- **value**: Specifies the maximum number of seconds between successive samples (interval value).

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>receiver_index</td>
<td>0</td>
</tr>
<tr>
<td>value</td>
<td>0</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the **no** form of this command to delete a poller.

### Examples

- `-> sflow poller 1 port 1/1/1 receiver 2 interval 20`
- `-> vrf vxlan sflow poller 1 port 1/1/1 receiver 2 interval 20`
- `-> sflow poller 1 port 1/2/6-10 receiver 1 interval 30`
- `-> no sflow poller 1 port 1/2/6-10`
Release History

Release 7.1.1; command was introduced.
Release 8.9R1; vrf parameter introduced.

Related Commands

show sflow poller Displays the poller table.

MIB Objects

sFlowCpTable
  sFlowCpDataSource
  sFlowCpInstance
  sFlowCpReceiver
  sFlowCpInterval
show sflow agent

Displays the sFlow agent table.

show sflow agent

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Released</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- It is necessary to execute the ip interface command to make a loopback0 IP address as the fixed primary address of the switch to avoid interface changes, which might need the collector software to be restarted for it to communicate using the new agent IP address. Normally, the primary IP address could change depending on the IP interface going up/down. Therefore, the sFlow agent always needs to send a fixed IP address in the datagram.

- The loopback address should be an IP interface configured on the switch.

Examples

-> ip interface loopback0 address 198.206.181.100
-> show sflow agent
Agent Version = 1.3; Alcatel; 6.1.1
Agent IP = 127.0.0.1

output definitions

<table>
<thead>
<tr>
<th>output definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Version</td>
<td>Identifies the version which includes the MIB version, organization name, and the specific software build of the agent.</td>
</tr>
<tr>
<td>Agent address</td>
<td>IP address associated with the agent. Configured through the sflow agent command.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Related Commands

show sflow receiver  Displays the receiver table.

MIB Objects

sFlowAgent
  sFlowVersion
  sFlowAgentAddressType
  sFlowAgentAddress
show sflow receiver

Displays the sFlow receiver table.

```
vrf {name} show sflow receiver [num]
```

**Syntax Definitions**

- **name**: The name of the VRF for which the sflow receiver table must be displayed.
- **num**: Specifies the receiver index.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show sflow receiver
Receiver 1
  Name       = Golden
  Address    = IP_V4  198.206.181.3
  UDP Port   = 6343
  Timeout    = 65535
  Packet Size= 1400
  DatagramVer= 5

-> show sflow receiver

Receiver 1
  Name       = Golden
  Address    = Domain Name  upam.omnivista.com IP_V4  198.206.181.3
  UDP Port   = 6343
  Timeout    = 65535
  Packet Size= 1400
  DatagramVer= 5
```
## output definitions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address of the sFlow collector. If a receiver address was configured as a domain name, then both the domain name and IP address for that domain are displayed. If the domain name did not translate to a valid IP address, a hyphen is displayed instead of an address.</td>
</tr>
<tr>
<td>UDP Port</td>
<td>Destination port for sFlow datagrams.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Time remaining before the sampler is released and stops sampling.</td>
</tr>
<tr>
<td>Packet size</td>
<td>Maximum number of data bytes that can be sent in a single sample datagram.</td>
</tr>
<tr>
<td>Datagram ver</td>
<td>Version of sFlow datagrams that should be sent.</td>
</tr>
</tbody>
</table>

## Release History

Release 7.1.1; command was introduced.
Release 8.9R1; `vrf` parameter introduced.

## Related Commands

- **sflow receiver**
  Sets the destination hosts where the sFlow datagrams are sent out.

## MIB Objects

- **sFlowRcvrTable**
  - **sFlowRcvrIndex**
**show sflow sampler**

Displays the sFlow sampler table.

```plaintext
vrf {name} show sflow sampler [num]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th><strong>name</strong></th>
<th>The name of the VRF for which the sflow sampler table must be displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>num</strong></td>
<td>Specifies the instance ID.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A.

### Examples

```plaintext
-> show sflow sampler
Instance   Interface    Receiver  Sample-rate   Sample-hdr-size
-----------------------------------------------------------------
1         2/1/1          1         2048             128
1         2/1/2          1         2048             128
1         2/1/3          1         2048             128
1         2/1/4          1         2048             128
1         2/1/5          1         2048             128
```

**output definitions**

<table>
<thead>
<tr>
<th><strong>Instance</strong></th>
<th>Instance for the flow sampler.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>Interface used for the flow sampler.</td>
</tr>
<tr>
<td><strong>Receiver</strong></td>
<td>Receiver associated with the flow sampler.</td>
</tr>
<tr>
<td><strong>Sample-rate</strong></td>
<td>Statistical sampling rate for packet sampling from the source.</td>
</tr>
<tr>
<td><strong>Sample-hdr-size</strong></td>
<td>Maximum number of bytes that should be copied from a sampled packet.</td>
</tr>
</tbody>
</table>
Release History
Release 7.1.1; command was introduced.
Release 8.9R1; vrf parameter introduced.

Related Commands
sflow sampler Gets hardware sampled from Q-dispatcher.

MIB Objects
sFlowFsTable
  sFlowFsInstance
**show sflow poller**

Displays the sFlow poller table.

```
show sflow poller [num]
```

### Syntax Definitions

- **name**: The name of the VRF for which the sflow poller table must be displayed.
- **num**: Specifies the instance ID.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6</th>
<th>6900 X48C6/T48C6-V48C8/C32E/T24C2/X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
$ show sflow poller
```

<table>
<thead>
<tr>
<th>Instance</th>
<th>Interface</th>
<th>Receiver</th>
<th>Interval(Secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2/1/6</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>1</td>
<td>2/1/7</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>1</td>
<td>2/1/8</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>1</td>
<td>2/1/9</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>1</td>
<td>2/1/10</td>
<td>1</td>
<td>30</td>
</tr>
</tbody>
</table>

**output definitions**

- **Instance**: Instance for the counter poller.
- **Interface**: Interface used for the counter poller.
- **Receiver**: Receiver associated with the counter poller.
- **Interval**: The maximum number of seconds between successive samples of the counters associated with the data source.
Release History

Release 7.1.1; command was introduced.
Release 8.9R1; vrf parameter introduced.

Related Commands

sflow poller          Gets counter samples.

MIB Objects

sFlowCpTable
  sFlowCpInstance
50  RMON Commands

Remote Network Monitoring (RMON) probes can be used to monitor, manage, and compile statistical data about network traffic from designated active ports in a LAN segment without negatively impacting network performance. This feature supports basic RMON 4 group implementation compliant with RFC 2819 (Remote Network Monitoring Management Information Base), but does not support RMON 10 group or RMON 2. This chapter includes descriptions of RMON commands used to enable or disable individual (or a group of a certain flavor type) RMON probes, show a list of (or individual) RMON probes and show a list of (or individual) RMON logged events.

MIB information for the RMON commands is as follows:

  Filename:  RMON-MIB.mib  
  Module:    rmonMibModule

The following table summarizes the available commands:

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>rmon probes</td>
</tr>
<tr>
<td>show rmon probes</td>
</tr>
<tr>
<td>show rmon events</td>
</tr>
</tbody>
</table>
rmon probes

This command enables or disables types of RMON probes.

```
rmon probes {stats | history | alarm} [entry_number] {enable | disable}
```

**Syntax Definitions**

- **stats**: Ethernet Statistics Table probe entries.
- **history**: History Control Table probe entries.
- **alarm**: Alarm Table probe entries.
- **entry_number**: The entry number in the list of probes (optional).
- **enable**: Enables the RMON probe.
- **disable**: Disables the RMON probe.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Network activity on subnetworks attached to the RMON probe can be monitored by NMS applications.
- RMON will not monitor activities on the CMM onboard Ethernet Management port.

**Examples**

- `rmon probes stats 4012 enable`
- `rmon probes history 10240 disable`
- `rmon probes alarm 11235 enable`
- `rmon probes stats enable`
- `rmon probes history disable`
- `rmon probes alarm enable`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **show rmon probes**: Displays a list of RMON probes or a single RMON probe.
- **show rmon events**: Displays a list of RMON logged events or a single RMON event.

MIB Objects

- **ETHERSTATSTABLE**
  - etherStatsStatus
- **HISTORYCONTROLTABLE**
  - historyControlStatus
- **ALARMTABLE**
  - alarmStatus
show rmon probes

Displays a list of RMON probes or a single RMON probe.

```
show rmon probes [stats | history | alarm] [entry_number]
```

Syntax Definitions

- **stats**: Ethernet Statistics Table probe entries.
- **history**: History Control Table probe entries.
- **alarm**: Alarm Table probe entries.
- **entry_number**: The entry number in the list of probes *(optional)*.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- To display a list of current probes, omit the *entry-number* from the command line.
- To display statistics for a particular probe, include the probe’s *entry_number* in the command line.
- The *show rmon probes* command displays the following information: Entry number, Slot/Port, Flavor (whether the probe type is Ethernet, History or Alarm), Status (Active or Inactive), Duration (time since the last change in status, in hours/minutes) and System Resources (the amount of memory allocated to this probe).
- The *show rmon probes entry-number* command displays the following information: Probe’s Owner (probe type and location), Slot/Port, Entry number, Flavor (whether the probe type is Ethernet, History or Alarm), Status (Active or Inactive), Time since the last change in status (hours/minutes), and System Resources (the amount of memory allocated to this probe). Displayed statistics may vary, depending on whether the probe type is Ethernet, History or Alarm.

Examples

```
-> show rmon probes stats

Chassis/
Entry  Slot/Port  Flavor  Status  Duration  System Resources
--------+----------+---------+---------+-----------+-----------------+
1026 1/1/26  Ethernet  Active  71:49:41  301 bytes
```

 OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 50-4
1025 1/1/25  Ethernet  Active      71:49:20     301 bytes
1001 1/1/1  Ethernet  Active      71:48:05     300 bytes

-> show rmon probes history

Chassis/
Entry  Slot/Port    Flavor    Status      Duration     System Resources
-------+----------+---------+-----------+------------+----------------
1     1/1/26     History   Active      71:50:08     5471 bytes
2     1/1/25     History   Active      71:49:47     5471 bytes
3     1/1/1      History   Active      71:48:32     5470 bytes
4     1/1/22     History   Active      71:48:30     5471 bytes
5     1/1/23     History   Active      71:48:30     5471 bytes

-> show rmon probes alarm

Entry Slot/Port Flavor Status Duration System Resources
-------+-----------+-----------+----------+---------------+---------------------
11235 1/4/8  Alarm Active 00:07:00 835 bytes

-> show rmon probes 4005

Probe's Owner: Switch Auto Probe on Chassis 1, Slot 4, Port 5, ifindex 4005
     Entry 4005
     Flavor = Ethernet, Status = Active,
     Time = 48 hrs 54 mins,
     System Resources (bytes) = 301

-> show rmon probes history 30562

Probe's Owner: Switch Auto Probe on Chassis 8, Slot 1, Port 29
History Control Buckets Requested = 50,
History Control Buckets Granted   = 50,
History Control Interval          = 30 seconds,
History Sample Index              = 287
     Entry 9
     Flavor = History, Status = Active,
     Time = 71 hrs 48 mins,
     System Resources (bytes) = 5471

-> show rmon probes alarm 11235

Probe's Owner:
Alarm Rising Threshold          = 5
Alarm Falling Threshold         = 0
Alarm Rising Event Index        = 26020
Alarm Falling Event Index       = 0
Alarm Interval                  = 10 seconds
Alarm Sample Type               = delta value
Alarm Startup Alarm             = rising alarm
Alarm Variable                  = 1.3.6.1.2.1.16.1.1.1.5.4008
     Entry 11235
     Flavor = Alarm, Status = Active
     Time = 48 hrs 48 mins,
     System Resources (bytes) = 1677
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe’s Owner</td>
<td>Description and interface (location) of the probe.</td>
</tr>
<tr>
<td>Slot/Port</td>
<td>The Slot/Port number (interface) that this probe is monitoring.</td>
</tr>
<tr>
<td>Entry</td>
<td>The Entry number in the list of probes.</td>
</tr>
<tr>
<td>Flavor</td>
<td>Whether the probe type is Ethernet, History, or Alarm.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the probe—<strong>Creating</strong> (the probe is under creation), <strong>Active</strong> (the probe is Active), or <strong>Inactive</strong> (the probe is inactive).</td>
</tr>
<tr>
<td>Duration</td>
<td>Elapsed time (hours/minutes/seconds) since the last change in status.</td>
</tr>
<tr>
<td>System Resources</td>
<td>Amount of memory that has been allocated to this probe.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `rmon probes` Enables or disables types of RMON probes.
- `show rmon events` Displays RMON logged events.

**MIB Objects**

- `ETHERSTATSTABLE`  
  - `etherStatsIndex`
- `HISTORYCONTROLTABLE`  
  - `historyControlIndex`
- `ALARMTABLE`  
  - `alarmIndex`
**show rmon events**

Displays RMON events (actions that take place based on alarm conditions detected by the RMON probe).

**show rmon events [entry_number]**

---

**Syntax Definitions**

*entry_number*  
The entry number in the list of probes *(optional).*

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- To display a list of logged events, omit the *entry_number* from the command line.
- To display statistics for a particular event, include the *entry_number* in the command line.
- The *show rmon events* command displays the following information for all RMON Logged Events:  
  Entry number, Time (hours/minutes/seconds) since the last change in status and Description (nature of the event).
- The *show rmon events entry_number* command displays the following information for a particular RMON Logged Event: Entry number, Time (hours/minutes/seconds) since the last change in status and Description (nature of the event).

**Examples**

```plaintext
-> show rmon events

<table>
<thead>
<tr>
<th>Entry</th>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00:08:00</td>
<td>etherStatsPkts.4008: [Falling trap] “Falling Event”</td>
</tr>
<tr>
<td></td>
<td>00:26:00</td>
<td>etherStatsCollisions.2008: “Rising Event”</td>
</tr>
</tbody>
</table>

-> show rmon events 2

<table>
<thead>
<tr>
<th>Entry</th>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>00:26:00</td>
<td>etherStatsCollisions.2008: “Rising Event”</td>
</tr>
</tbody>
</table>
```
**output definitions**

<table>
<thead>
<tr>
<th>Entry</th>
<th>The entry number in the list of probes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Time (hours, minutes, and seconds) since the last change in status.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the Alarm condition detected by the probe.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `rmon probes` Enables or disables types of RMON probes.
- `show rmon probes` Displays RMON probes or a single RMON probe.

**MIB Objects**

EVENTTABLE

- `eventIndex`
This chapter includes descriptions for Switch Logging commands. These commands are used to configure parameters for the Switch Logging utility.

MIB information for the system commands is as follows:

- **Filename:** ALCATEL-IND1-SYSTEM-MIB.mib
- **Module:** alcatelIND1SystemMIB

A summary of the available commands is listed here.

```
swlog
swlog syslog-facility-id
swlog appid
swlog output
swlog output flash-file-size
swlog advanced
swlog size-trap-threshold
swlog clear
show log swlog
show swlog
swlog console level
show log events
show log events output
```
swlog

Enables or disables switch logging. Switch logging allows you to view a history of various switch activities in a text format.

swlog {enable | disable | preamble | hash-time-limit seconds | duplicate-detect | console level num }

no swlog [preamble | duplicate-detect]

Syntax Definitions

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of the command to enable or disable the preamble and duplicate-detect setting.
- The syslog preamble includes the level, appid, and timestamp that precedes the actual log messages.
- If duplicate entries are received within the configured hash-time-limit, only a single entry will be logged along with the number of times duplicated.
• Use the `swlog console level` command to set the switch logs of different levels to be displayed on the console.

**Examples**

-> swlog enable
-> swlog hash-time-limit 30
-> no swlog preamble

**Release History**

Release 7.1.1; command was introduced.
Release 8.3.1.R02; `gmt-time` parameter added.
Release 8.4.1; `gmt-time` parameter removed.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>swlog appid</code></td>
<td>Defines the level at which switch logging information will be filtered for</td>
</tr>
<tr>
<td></td>
<td>the specified application.</td>
</tr>
<tr>
<td><code>swlog output</code></td>
<td>Enables or disables switch logging output to the console, file, or data</td>
</tr>
<tr>
<td></td>
<td>socket.</td>
</tr>
<tr>
<td><code>show log swlog</code></td>
<td>Displays stored switch logging information from flash.</td>
</tr>
<tr>
<td><code>show swlog</code></td>
<td>Displays switch logging information.</td>
</tr>
<tr>
<td><code>swlog console level</code></td>
<td>Allows to set the switch logs of different levels to be displayed on the</td>
</tr>
<tr>
<td></td>
<td>console. All application events of defined level and lower are displayed</td>
</tr>
<tr>
<td></td>
<td>on the console.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- `systemSwitchLogging`
- `systemSwitchLoggingEnable`
- `systemSwitchLoggingPreamble`
- `systemSwitchLoggingHashAgeLimit`
- `systemSwitchLoggingDuplicateDetect`
- `systemSwitchLoggingConsoleLevel`
- `systemSwitchLoggingGmtTime`
**swlog syslog-facility-id**

Specifies a facility ID that switch logging includes in the priority (PRI) section of the event message.

```
swlog syslog-facility-id {facility_id | num}
```

### Syntax Definitions

- **facility_id**
  - A facility identification keyword. Current facility IDs are listed in the table below.
- **num**
  - A numerical equivalent value for the facility ID. The range is 0–23. Current numeric equivalent values are listed in the table below.

### Supported Facility IDs with Numerical Equivalents

<table>
<thead>
<tr>
<th>Facility ID</th>
<th>Numerical Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>kernel - 0</td>
<td>NTP - 12</td>
</tr>
<tr>
<td>user - 1</td>
<td>log-audit - 13</td>
</tr>
<tr>
<td>mail - 2</td>
<td>log-alert - 14</td>
</tr>
<tr>
<td>system - 3</td>
<td>clock2 - 15</td>
</tr>
<tr>
<td>sec-auth1-2</td>
<td>local0 - 16</td>
</tr>
<tr>
<td>syslog - 5</td>
<td>local1 - 17</td>
</tr>
<tr>
<td>lptr - 6</td>
<td>local2 - 18</td>
</tr>
<tr>
<td>net-news - 7</td>
<td>local3 - 19</td>
</tr>
<tr>
<td>UUCP - 8</td>
<td>local4 - 20</td>
</tr>
<tr>
<td>clock1-9</td>
<td>local5 - 21</td>
</tr>
<tr>
<td>sec-auth2 - 10</td>
<td>local6 - 22</td>
</tr>
<tr>
<td>FTP - 11</td>
<td>local7 - 23</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>facility_id</td>
<td>local0</td>
</tr>
<tr>
<td>num</td>
<td>16</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the ID name (system) or the numeric equivalent to specify the facility ID.
Examples

-> swlog syslog-facility-id system
-> swlog syslog-facility-id 3
-> swlog syslog-facility-id user
-> swlog syslog-facility-id 1

Release History

Release 8.3.1; command introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>swlog</td>
<td>Enables or disables switch logging.</td>
</tr>
<tr>
<td>show log swlog</td>
<td>Displays stored switch logging information from flash.</td>
</tr>
<tr>
<td>show swlog</td>
<td>Displays switch logging information.</td>
</tr>
</tbody>
</table>

MIB Objects

systemSwitchLogging
  systemSwitchLoggingSysLogFacilityId
swlog appid

Defines the level at which switch logging information will be filtered for the specified application. All application events of the defined level and lower are captured.

swlog appid {all | string} {library {all | string} | subapp {all | num} | exclude {all | num}} {disable | enable} level {level | num} [vrf num]

Syntax Definitions

string
An application or library identification keyword. Enter a question mark (?) on the command line to get a list of application or library IDs.

subapp num
A numerical equivalent value for the subapp ID. Enter a question mark (?) on the command line to get a list of subapp IDs.

exclude num
A numerical equivalent value for the subapp ID. Enter a question mark (?) on the command line to get a list of subapp IDs.

disable
Disables the logging of the associated application.

enable
Enables the logging of the associated application.

level level | num
The severity level filter keyword or numerical equivalent value for the application ID (see table below). All switch logging messages of the specified level and lower will be captured. The severity level is a value assigned to the relative severity of the switch logging message. A lower value indicates messages that are more severe, a higher value indicates messages that are less severe.

vrf num
The VRF ID.

<table>
<thead>
<tr>
<th>Supported Levels</th>
<th>Numeric Equivalents</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>0</td>
<td>Disabled</td>
</tr>
<tr>
<td>alarm</td>
<td>1</td>
<td>Highest severity. The system is about to crash and reboot.</td>
</tr>
<tr>
<td>error</td>
<td>2</td>
<td>System functionality is reduced.</td>
</tr>
<tr>
<td>alert</td>
<td>3</td>
<td>A violation has occurred.</td>
</tr>
<tr>
<td>warning</td>
<td>4</td>
<td>A unexpected, non-critical event has occurred.</td>
</tr>
<tr>
<td>event</td>
<td>5</td>
<td>A clear readable customer event.</td>
</tr>
<tr>
<td>info</td>
<td>6</td>
<td>Any other non-debug message (default).</td>
</tr>
<tr>
<td>debug1</td>
<td>7</td>
<td>A normal event debug message.</td>
</tr>
<tr>
<td>debug2</td>
<td>8</td>
<td>A debug-specific message.</td>
</tr>
<tr>
<td>debug3</td>
<td>9</td>
<td>All debug messages.</td>
</tr>
</tbody>
</table>

Defaults

Default severity level is info.
Switch Logging Commands

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td></td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `show swlog appid` command to display available registered applications.
- Specify the `event` severity level keyword to define the new event level at which switch logging information will be filtered for the specified application.

Examples

- `swlog appid all subid all enable`
- `swlog appid mvrpNi subapp 1 level 8`
- `swlog appid all supapp all level event`
- `swlog appid all library all level event`
- `swlog appid all exclude all level event`
- `show swlog appid mvrpNi`

Application Name : mvrpNi,

<table>
<thead>
<tr>
<th>SubAppl ID Sub Application Name</th>
<th>Level</th>
<th>VRF Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>main</td>
<td>error</td>
<td>VRF 1-64 info</td>
</tr>
</tbody>
</table>

- `swlog appid ?`

- `swlog appid udprelay library ?`

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 51-7
Switch Logging Commands

swlog appid

tcamlibcmm esmLib ipms_client ipmc_idx
mirApiLibCMM ipcmmLib qos mplscore routemap

-> swlog appid udprelay subapp ?
   ^
   ALL <num> <string>
   1=main 2=dhcp-snooping 3=tcam

-> swlog appid udprelay exclude ?
   ^
   ALL <num> <string>
   1=main 2=dhcp-snooping 3=tcam

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; exclude parameter added.
Release 8.6.R1; event severity level keyword added.

Related Commands

swlog Enables or disables switch logging.
swlog output Enables or disables switch logging output to the console, file, or data socket.
show log swlog Displays stored switch logging information from flash.
show swlog Displays switch logging information.
swlog console level Allows to set the switch logs of different levels to be displayed on the console. All application events of defined level and lower are displayed on the console.

MIB Objects

systemSwitchLogging
    systemSwitchLoggingAppName
    systemSwitchLoggingLibraryName
    systemSwitchLoggingLevel
**swlog output**

Enables or disables switch logging output to the console, file, data socket (remote session), or external syslog server.

```bash
swlog {host | ni} [slot chassis/slot] output {tty {enable | disable} | console | flash | socket {ip_address [port] | ipv6Address [port] | domain_name | console {enable | disable}} [tls] [remote command-log] [vrf-name name]}
```

```bash
no swlog output {console | flash | socket [ip_address | ipv6Address | domain_name]}
```

**Syntax Definitions**

- **tty enable**
  Enables switch logging to a connected Telnet session.

- **tty disable**
  Disables switch logging to a connected Telnet session.

- **host**
  Enable or disable host logging to remote syslog server.

- **ni**
  Enable or disable NI logging to remote syslog server.

- **slot chassis/slot**
  The chassis ID and slot ID of the NI output socket.

- **console**
  Specifies console output. When enabled, switch logging output is printed to the user console.

- **flash**
  Specifies /flash file output. When enabled, switch logging output is printed to a file in the switch’s /flash file system.

- **socket**
  Specifies data socket output. When enabled, switch logging output is printed to a remote session.

- **ip_address**
  The IPv4 address for the remote session host.

- **ipv6Address**
  The IPv6 address for the remote session host.

- **port**
  The socket port number.

- **domain_name**
  A Fully Qualified Domain Name (FQDN) for the remote session host. Specify a domain name up to 128 characters in length.

- **console enable**
  Enables uploading of the console log(s) to the remote syslog server.

- **console disable**
  Disables uploading of the console log(s) to the remote syslog server.

- **tls**
  Enables or disables syslog over TLS.

- **remote command-log**
  Enables command logging to a remote session host.

- **name**
  Specifies the VRF to be used to access the remote syslog server.
Switch Logging Commands

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>console</td>
<td>flash and console</td>
</tr>
<tr>
<td>flash</td>
<td></td>
</tr>
<tr>
<td>socket</td>
<td></td>
</tr>
<tr>
<td>console {enable</td>
<td>disable}</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the **no** form of this command to disable one or more configured output IP addresses.
- This command can also be used on the secondary CMM.
- Use the **socket** keyword to send output to a syslog server, followed by the IP address or FQDN of the remote host. Up to 12 servers can be configured. When an FQDN is specified, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.
- To enable uploading of console logs to a remote syslog server, it is mandatory to have at least one remote syslog server configured (**swlog output socket <ip_address>**). If there is no UDP remote syslog server configured, an error message will be displayed.
- To enable host and NI logging to remote syslog server, it is mandatory to have at least one remote syslog server configured (**swlog output socket <ip_address>**).
- The host and NI logging to remote syslog server is supported only on OS9900.
- When all the configured remote syslog server is removed, the status of all NI and host remote logging is automatically set to disabled.
- Syslog over TLS:
  - Remote command log will not work when syslog over TLS is enabled.
  - VRF cannot be used to access the syslog server when syslog over TLS is enabled.
  - In OmniSwitch 9900 only CMM swlog is transferred to the external syslog server over TLS.
  - Dying Gasp syslog messages are not captured in syslog over TLS.
  - Use the **no** form of the command to disable syslog over TLS.
- VRF name must either be ‘default’ or a pre-defined VRF (user-defined).

Examples

- `-> swlog output console`
- `-> no swlog output flash`
Switch Logging Commands

swlog output

- swlog output socket 14.1.1.1
- swlog output socket 14.1.1.2 1234
- swlog output socket console enable
- swlog host output socket enable
- swlog host output socket disable
- swlog ni slot 1/3 output socket enable
- swlog ni slot 2/3 output socket disable
- swlog output socket 14.1.1.1 remote command-log
- swlog output socket 14.1.1.1 vrf-name vrf1
- no swlog output socket 14.1.1.1

- swlog output socket upam.omnivista.com
- swlog output socket upam.omnivista.com remote command-log
- swlog output socket upam.omnivista.com vrf-name vrf1
- no swlog output socket upam.omnivista.com
- swlog output socket opendaylight.com
ERROR: DNS lookup failed, unknown host opendaylight.com
- swlog output socket 192.168.120.140 tls
- swlog output socket 2001::1 tls
- no swlog output socket 2001::1

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; vrf-name parameter added.
Release 8.3.1; remote command-log parameter added.
Release 8.5R1; domain_name parameter option added.
Release 8.6R1; tls parameter added.
Release 8.8R1; host, ni, console {enable | disable} parameter added.

Related Commands

swlog Enables or disables switch logging.
swlog appid Defines the level at which switch logging information will be filtered for the specified application.
show log swlog Displays stored switch logging information from flash.
show swlog Displays switch logging information.

MIB Objects

systemSwitchLogging
  systemSwitchLoggingTty
  systemSwitchLoggingFlash
  systemSwitchLoggingSocket
  systemSwitchLoggingSocketIpAddr
  systemSwitchLoggingConsole
  systemSwitchLoggingOutputSocketConsole
  systemSwitchLoggingHostOutputSocket
  systemSwitchLoggingNiOutputSocketEnable
  systemSwitchLoggingHostTable
  systemSwitchLoggingHostIpAddr
  systemSwitchLoggingHostPort
  systemSwitchLoggingHostStatus
  systemSwitchLoggingHostUserCommandHost
systemSwitchLoggingHostVrfName
systemSwitchLoggingHostDnTable
  systemSwitchLoggingHostDnName
  systemSwitchLoggingHostDnPort
  systemSwitchLoggingHostDnUserCommandHost
  systemSwitchLoggingHostDnVrfName
  systemSwitchLoggingHostDnStatus
  systemSwitchLoggingHostTls
swlog output flash-file-size

Configures the size of the switch logging file.

**swlog output flash-file-size kilobytes**

---

### Syntax Definitions

**kilobytes**  
The size of the switch logging file in kilobytes. The range is 125–12500.

---

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>kilobytes</td>
<td>1250</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6900V</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- Use the **show hardware-info** command to determine the amount of available flash memory.
- This command can also be used on the secondary CMM.

---

### Examples

```
-> swlog output flash-file-size 256
```

---

### Release History

Release 7.1.1; command was introduced.
Related Commands

- **swlog advanced**  
  Clears the files that store switch logging data.
- **show log swlog**  
  Displays stored switch logging information from flash.
- **show swlog**  
  Displays switch logging information.

MIB Objects

- **systemSwitchLogging**
  - **systemSwitchLoggingFileSize**
**swlog advanced**

Enable or disable switch logging in RFC5424 format.

```
swlog advanced {enable | disable}
```

---

**Syntax Definitions**

- **enable**: Enable switch logging in RFC5424 format.
- **disable**: Disable switch logging in RFC5424 format.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- By default, the switch logs the messages in BSD syslog format (RFC3164) to files and remote syslog servers.

- When switch logging RFC5424 format is enabled, the old RFC3164 syslog messages are reformatted to comply with the RFC5424 before writing to files or sending to remote syslog servers.

---

**Examples**

```
-> swlog advanced enable
-> swlog advanced disable
```

---

**Release History**

Release 8.4.1; command introduced.
**Related Commands**

**show swlog**
Displays switch logging information.

**MIB Objects**

```mib
systemSwitchLoggingSyslogProtocol
```
**swlog size-trap-threshold**

Configures the threshold limit of the storage space used for swlog record storage. When the storage reaches the configured threshold limit a notification is displayed in the swlog message.

**swlog size-trap-threshold** *threshold*

---

### Syntax Definitions

*threshold* The percentage of storage space to be set as threshold limit. The valid range is 50–90.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>90</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- Use this command to configure the threshold limit of the storage space used for swlog record storage.
- Use the **swlog clear** command to clear the files that store switch logging data.

---

### Examples

-> swlog size-trap-threshold 90

---

### Release History

Release 8.4.1; command introduced.
Related Commands

swlog clear  Clears the files that store switch logging data.
show log swlog  Displays stored switch logging information from flash.
show swlog  Displays switch logging information.

MIB Objects

systemSwitchLoggingSizeTrapThreshold
swlog clear

Clears the files that store switch logging data.

swlog clear [all]

Syntax Definitions

all

Clears all the contents of the switch log file.

Defaults

By default, the contents of the switch log file is cleared but the event logs are retained.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>supported</th>
<th>supported</th>
<th>supported</th>
<th>supported</th>
<th>supported</th>
<th>supported</th>
<th>supported</th>
<th>supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>66570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C4/E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C32/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use this command when the switch logging display is too long due to some of the data being old or out of date.
- This command can also be used on the secondary CMM.
- To clear all the contents including the event log use the “all” parameter with swlog clear command.

Examples

-> swlog clear
-> swlog clear all

Release History

Release 7.1.1; command was introduced.
Release 8.6R2; all parameter added.
Related Commands

- **swlog output**: Enables or disables switch logging output to the console, file, or data socket.
- **show log swlog**: Displays stored switch logging information from flash.
- **show swlog**: Displays switch logging information.

MIB Objects

- **systemSwitchLogging**
- **systemSwitchLoggingClear**
**show log swlog**

Displays stored switch logging information.

```
show log swlog
show log swlog [timestamp mm/dd/yyyy hh:mm:ss] [slot num] [reverse]
```

**Syntax Definitions**

- `mm/dd/yyyy hh:mm:ss`: Specify the starting time for the switch logging information to be displayed. Use the format `mm/dd/yyyy hh:mm:ss` where `mm` represents the month, `dd` is the day, `yyyy` is the year, `hh` is the hour, `mm` is the minutes and `ss` is the seconds. Use four digits to specify the year.

- `num`: The slot number to display the logging information for. *Currently not supported.*

- `reverse`: Display logs from the most recent to the oldest in time order of log files. `/flash/`.

**Default**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Compatibility</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the switch logging display is too long, you may use the `swlog advanced` command to clear all of the switch logging information.

- The use of `grep` and the `timestamp` parameter can be used to filter the log files.

- When the switch is in ASA enhanced mode, both user name and password is prompted to view the SWLOG data using `show log swlog` command. Only those users who provide the valid ASA credentials are allowed to view the data. For more information on Authenticated Switch Access - Enhanced Mode mode, refer to the “Managing Switch Security” chapter in *OmniSwitch AOS Release 8 Switch Management Guide.*

**Examples**

```
-> show log swlog timestamp 09/30/2011 13:27:00
Displaying file contents for '/flash/swlog.6'
```
Switch Logging Commands

Displaying file contents for '/flash/swlog.5'
<output truncated>

Sep 30 13:27:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

-> show log swlog | grep ChassisSupervisor
Displaying file contents for '/flash/swlog.6'
Displaying file contents for '/flash/swlog.5'
<output truncated>

Sep 28 13:25:15 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

Sep 30 13:26:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

Sep 30 13:27:16 Chassis6900 local0.info swlogd: ChassisSupervisor fan & temp Mgr info(5) Alert: PS1 airFlow unknown yet- duplicated 5 times!

When the switch is in ASA enhanced mode, both user name and password is prompted to view the SWLOG data using show log swlog command.

-> show log swlog
Username: test
Password: ********

show log swlog | grep error and show log swlog | grep more commands are not supported in enhanced mode.

Release History

Release 7.1.1; command was introduced.

Related Commands

- **swlog**
  Enables or disables switch logging.
- **swlog appid**
  Adds or removes a filter level for a specified subsystem.
- **swlog output**
  Enables or disables switch logging output to the console, file, or data socket.
- **swlog advanced**
  Clears the files that store switch logging data.
- **show swlog**
  Displays switch logging information.

MIB Objects

| N/A |
**show swlog**

Displays switch logging information (for example, switch logging status, log devices, application IDs with non-default severity level settings).

```
show swlog [library | appid {all | string} | dying-gasp-station]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>library</td>
<td>Displays the entire library for all application IDs.</td>
</tr>
<tr>
<td>string</td>
<td>The name of the application ID to display. Enter a question mark (?) on the command line to get a list of application IDs.</td>
</tr>
<tr>
<td>dying gasp-station</td>
<td>Displays switch logging information for Dying Gasp entries.</td>
</tr>
</tbody>
</table>

### Defaults

By default, the switch logging configuration for the switch is displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command can also be used on the secondary CMM.

### Examples

```
-> show swlog
Operational Status                 : Running,
File Size per file                 : 1250 Kbytes,
Log Device 1                       : console flash socket,
Log Device 2                       : ipaddr 10.2.2.1 remote command-log,
Syslog FacilityID                  : local0(16),
Hash Table entries age limit       : 60 seconds,
Switch Log Preamble                : Enabled,
Switch Log Debug                   : Disabled,
Switch Log Duplicate Detection     : Enabled,
Console Display Level              : debug1,
RFC5424 Format Logging             : Enabled,
Swlog Threshold                    : 90 percent
Syslog over TLS                    : Enabled
Host output socket                 : Enabled,
Output Socket Console              : Enabled,
Chassis 1 NI Output socket:        
    NI 3                             : Enabled,
```
Switch Logging Commands

show swlog

<table>
<thead>
<tr>
<th>SubAppId</th>
<th>ID Sub Application Name</th>
<th>Level</th>
<th>VRF Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>main</td>
<td>info</td>
<td>VRF 1-1024 info</td>
</tr>
<tr>
<td>2</td>
<td>dhcp-snooping</td>
<td>info</td>
<td>VRF 1-1024 info</td>
</tr>
<tr>
<td>3</td>
<td>tcam</td>
<td>info</td>
<td>VRF 1-1024 info</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Operational Status</th>
<th>Displays whether switch logging is enabled or disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Size per file</td>
<td>The maximum file size of the switch log file.</td>
</tr>
<tr>
<td>Log Device</td>
<td>Which devices are the switch log messages being sent to.</td>
</tr>
<tr>
<td>Log Device</td>
<td>Which devices are the switch log messages being sent to.</td>
</tr>
<tr>
<td>Syslog FacilityID</td>
<td>The Facility ID value that is included in the priority (PRI) section of the event messages.</td>
</tr>
<tr>
<td>Hash Table entries age limit</td>
<td>The elapsed time for duplicate entries.</td>
</tr>
<tr>
<td>Switch Log Preamble</td>
<td>Status of displaying message preamble on console.</td>
</tr>
<tr>
<td>Switch Log Debug</td>
<td>Status of swlog debug.</td>
</tr>
<tr>
<td>Switch Log Duplicate Detection</td>
<td>Status of duplicate detection.</td>
</tr>
<tr>
<td>Console Display Level</td>
<td>The console severity level.</td>
</tr>
<tr>
<td>RFC5424 Format Logging</td>
<td>Displays if switch logging in RFC5424 format is enabled or disabled.</td>
</tr>
<tr>
<td>Swlog Threshold</td>
<td>Displays the configured threshold limit for swlog record storage.</td>
</tr>
<tr>
<td>Syslog over TLS</td>
<td>Displays the operational status of syslog over TLS.</td>
</tr>
<tr>
<td>Host output socket</td>
<td>Displays if host logging to remote syslog server is enabled or disabled.</td>
</tr>
<tr>
<td>Application Name(id)</td>
<td>The subsystem information for the Application ID.</td>
</tr>
<tr>
<td>Output Socket Console</td>
<td>Displays whether uploading of console log to remote syslog server is enabled or disabled.</td>
</tr>
<tr>
<td>NI output socket</td>
<td>Displays if NI logging to remote syslog server is enabled or disabled. It also displays the chassis ID and slot ID on which it is enabled.</td>
</tr>
</tbody>
</table>
Switch Logging Commands

-> show swlog appid ?

ALL <string>
SWLOG PMD ChassisSupervisor flashManager MIP_GATEWAY
ConfigManager capManCmm vc_licManager vcmCmm SSTIME SSAPP
mrvid capManSig fabric portMgrCmm vfcm intfCmm dafCmm
linkAggCmm VlanMgrCmm ipmscmm pvlanCmm isis_spb_0 isisVc
stpCmm AGCM C mm mi rMonSF l owCmm ipv4 ipv6 ipsecSys ipsec
tcamCmm qosCmm vstkCmm eoamCmm erpCmm NT P udpRelay
remoteConfig AAA havlanCmm SES rmon WEBVIEW trapmgr radCli
ldapClientCmm tacClientCmm healthCmm svcCmm lldpCmm udldCmm
mpls ssaCmm SNMP csEventMonitor bfdCmm mvrpCmm
dhcp6r messageService dhcp6srv dhcpSrv grm bcdCmm lpCmm
DG_CMM qmrCmm iprm_0 vrrp_0 ospf_0 flashManagerNI capManNi
vcmCmm portMgrNI bcd vfCm intfsCmm dafCmni linkAggNI VlanMgrNI
stpNI erpNI vstkNI fdbmgr1 slNI healthNI ipni ip6ni
mirMonSF l owNI tcannI qosNI ipmsNI svcNI lldpNI udldNI
bfdni mvrpNI AGNI DG_NI nipktrly loamNI eoamNI fdbmgr4 lpNI
fdbmgr3

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; dying-gasp-station parameter added.
Release 8.3.1.R02; GMT time logging field added.
Release 8.4.1; GMT time logging field replaced with RFC5424 Format Logging. Swlog Threshold.
Release 8.6R1; Syslog over TLS field added in show swlog output.
Release 8.8R1; Host output socket, Output Socket Console, NI output socket field added in show swlog output.

Related Commands

swlog Enables or disables switch logging.
slog syslog-facility-id Configures the value of the facility ID that switch logging includes in the priority (PRI) section of the event message.
swlog appid Defines the level at which switch logging information will be filtered for the specified application.
swlog output Enables or disables switch logging output to the console, file, or data socket.
swlog output flash-file-size Configures the size of the switch logging file.
swlog size-trap-threshold Configures the threshold limit of the storage space used for swlog record storage.
show log swlog Displays stored switch logging information from flash.
show log events Displays customer event logs on the switch.
show log events output Captures all event log to a specified file name on the switch.
MIB Objects

systemSwitchLogging
  systemSwitchLoggingEnable
  systemSwitchLoggingPreamble
  systemSwitchLoggingHashAgeLimit
  systemSwitchLoggingDuplicateDetect
  systemSwitchLoggingConsoleLevel
  systemSwitchLoggingGmtTime
  systemSwitchLoggingSysLogFacilityId
  systemSwitchLoggingAppName
  systemSwitchLoggingLibraryName
  systemSwitchLoggingLevel
  systemSwitchLoggingTty
  systemSwitchLoggingFlash
  systemSwitchLoggingSocket
  systemSwitchLoggingSocketIpAddr
  systemSwitchLoggingConsole
  systemSwitchLoggingFileSize
  systemSwitchLoggingSyslogProtocol
  systemSwitchLoggingSizeTrapThreshold
  systemSwitchLoggingHostOutputSocket
  systemSwitchLoggingNiOutputSocketEnable
systemSwitchLoggingHostTable
  systemSwitchLoggingHostIpAddr
  systemSwitchLoggingHostPort
  systemSwitchLoggingHostStatus
  systemSwitchLoggingHostUserCommandHost
  systemSwitchLoggingHostVrfName
  systemSwitchLoggingHostTls
systemSwitchLoggingDgHostTable
  systemSwitchLoggingDgHostIndex
  systemSwitchLoggingDgHostIpType
  systemSwitchLoggingDgHostIpAddr
**swlog console level**

Allows to set the switch logs of different levels to be displayed on the console. All application events of defined level and lower are displayed on the console.

```
swlog console level {num | alarm | alert | debug1 | debug2 | debug3 | error | info | off | warning }
```

### Syntax Definitions

- **console level num**
  The severity level filter keyword or numeric value for the application ID. *(see table for swlog appid command)*.
- **alarm**
  Sets the log level to display highest severity. *(The system is about to crash and reboot)*
- **alert**
  Sets the log level to display on console when a violation has occurred.
- **debug1**
  Sets the log level to display normal event debug message to be displayed on console.
- **debug2**
  Sets the log level to display a debug-specific message to be displayed on console.
- **debug3**
  Sets the log level to display all debug messages on the console.
- **error**
  Sets the log level to display on console when system functionality is reduced.
- **info**
  Sets the log level to display any other non-debug message on the console.
- **off**
  Sets the log level as disabled. No logs are displayed on the console.
- **warning**
  Sets the log level to display on console when an unexpected, non-critical event has occurred.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>console level num</td>
<td>6 (info)</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/N48C8</th>
<th>C32E/T24C2</th>
<th>X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `show swlog` command to display the console display level.
**Examples**

-> swlog console level 5  
-> swlog console level info

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **swlog appid**
  Defines the level at which switch logging information will be filtered for the specified application.

- **swlog output**
  Enables or disables switch logging output to the console, file, or data socket.

- **show log swlog**
  Displays stored switch logging information from flash.

- **show swlog**
  Displays switch logging information.

- **show log events**
  Displays customer event logs on the switch.

- **show log events output**
  Captures all event log to a specified file name on the switch.

**MIB Objects**

- **systemSwitchLogging**
  - **systemSwitchLoggingConsoleLevel**
**show log events**

Displays customer event logs on the switch.

```plaintext
show log events
```

## Syntax Definitions

N/A

## Defaults

N/A

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Use this command to display customer event logs.

## Examples

```
-> show log events
2019 Apr 28 19:17: 8.83  : CMM : ChassisSupervisor : chassisTrapsAlert - CERTIFY w/FLASH SYNCHRO process started
2019 Apr 28 19:25:25.303 : CMM : ChassisSupervisor : The switch was restarted by the user
```

## output definitions

The log output is in the following format:

```
<SWLOG TIMESTAMP> : <CMM>/<NI> : <MODULE_NAME> : <LOG_DESCRIPTION>
```
Release History

Release 8.6R1; command was introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show log events output</td>
<td>Captures all event log to a specified file name on the switch.</td>
</tr>
<tr>
<td>swlog output</td>
<td>Enables or disables switch logging output to the console, file, or data socket.</td>
</tr>
<tr>
<td>show log swlog</td>
<td>Displays stored switch logging information from flash.</td>
</tr>
<tr>
<td>show swlog</td>
<td>Displays switch logging information.</td>
</tr>
</tbody>
</table>

MIB Objects

| N/A |
show log events output

Captures all event log to a specified file name on the switch.

**show log events output** filename

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to capture all event log to a filename.
- All the logs related to customer events will be appended “CUSTLOG” to the prefix to differentiate events from normal debug logs.

**Examples**

-> show log events output /flash/myevents

**Release History**

Release 8.6R1; command was introduced.
Related Commands

**show log events**  Displays customer event logs on the switch.

**swlog output**  Enables or disables switch logging output to the console, file, or data socket.

**show log swlog**  Displays stored switch logging information from flash.

**show swlog**  Displays switch logging information.

MIB Objects

| N/A |
The Health Monitoring function monitors the consumable resources of the switch (for example, bandwidth usage, CPU usage) and provides a single integrated resource for a Network Management System (NMS). This function monitors the switch, and at fixed intervals, collects the current values for each resource being monitored. Users specify resource threshold limits and traps are sent to an NMS if a value falls above or below a user-specified threshold.

The Health Monitoring commands comply with RFC1212.

MIB information for the Health Monitoring commands is as follows:

Filename: ALCATEL-IND1-HEALTH-MIB.mib
Module: alcatelIND1HealthMonitorMIB

A summary of the available commands is listed here:

- `health threshold`
- `health interval`
- `show health configuration`
- `show health`
- `show health all`
**health threshold**

Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, CPU usage, and flash usage.

Input traffic, output/input traffic, memory usage, and CPU usage thresholds specify the maximum percentage for each resource that may be consumed before a trap is sent to the user.

```
health threshold {rx percent | txrx percent | memory percent | cpu percent | flash percent}
```

**Syntax Definitions**

- **rx** Specifies the maximum input (RX) traffic threshold.
- **txrx** Specifies the maximum output/input (TX/RX) traffic threshold.
- **memory** Specifies the maximum RAM memory usage threshold.
- **cpu** Specifies the maximum CPU usage threshold.
- **flash** Specifies the maximum flash usage threshold.
- **percent** The new threshold value, in percent, for the corresponding resource (rx, txrx, memory, cpu, flash). The valid range is 1–100.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>percentage</td>
<td>80</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When a resource falls back below the configured threshold, an additional trap is sent to the user. This indicates that the resource is no longer operating beyond its configured threshold limit.

- Changing a threshold value sets the value for all levels of the switch (the switch, module, and port). You cannot set different threshold values for each level.

- For detailed information on each threshold type, refer to page 52-5, or refer to the chapter titled “Diagnosing Switch Problems” in the OmniSwitch AOS Release 8 Network Configuration Guide.

- To view the current health threshold values, use the `show health configuration` command.
Examples

-> health threshold rx 85
-> health threshold txrx 55
-> health threshold memory 95
-> health threshold cpu 85

Release History

Release 7.1.1; command introduced.

Related Commands

show health configuration Displays the current health threshold settings.

MIB Objects

HealthThreshInfo
  healthThreshDeviceRxLimit
  healthThreshDeviceTxRxLimit
  healthThreshDeviceMemoryLimit
  healthThreshDeviceCpuLimit
  healthThreshFlashLimit
**health interval**

Configures the sampling interval between health statistics checks. The sampling interval is the time interval between polls of the consumable resources of the switch to see if it is performing within set thresholds.

**health interval seconds**

**Syntax Definitions**

`seconds` Sampling interval (in seconds). Valid entries are 10, 12, 15, 20, 30.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>10</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Decreasing the polling interval may impact switch performance.

**Examples**

-> health interval 20

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`show health` Displays the current health sampling interval.

**MIB Objects**

HealthThreshInfo

  healthSamplingInterval
**show health configuration**

Displays current health configuration settings.

```
show health configuration
```

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show health configuration
Rx Threshold = 80,
TxRx Threshold = 80,
CPU Threshold = 80,
Memory Threshold = 80,
Flash Threshold = 80,
Sampling Interval (Secs) = 10
```
**output definitions**

| **Rx Threshold** | The current device input (RX) threshold. This value displays the maximum percentage of total bandwidth allowed for incoming traffic on the switch. The total bandwidth is defined as the Ethernet port capacity for all NI modules currently operating in the switch, in Mbps. For example, a chassis with 48 100Base-T Ethernet ports installed has a total bandwidth of 4800 Mbps. The default value is 80 percent and can be changed using the `health threshold` command. |
| **TxRx Threshold** | The current device output/input (TX/RX) threshold. This value displays the maximum percentage of total bandwidth allowed for all incoming and outgoing traffic. As with the RX threshold described above, the total bandwidth is defined as the Ethernet port capacity for all the NI modules currently operating in the switch, in Mbps. The default value is 80 percent and can be changed using the `health threshold` command. |
| **CPU Threshold** | Displays the current CPU usage threshold. CPU usage refers to the total amount of CPU processor capacity currently used by switch applications. The default value is 80 percent and can be changed using the `health threshold` command. |
| **Memory Threshold** | Displays the current memory usage threshold. Memory usage refers to the total amount of RAM memory currently used by switch applications. The default value is 80 percent and can be changed using the `health threshold` command. |
| **Flash Threshold** | Displays the current flash usage threshold. The default value is 80 percent and can be changed using the `health threshold` command. |
| **Sampling Interval** | Displays the sampling interval time period in seconds. Sampling interval can be changed using the `health interval` command. |

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `health threshold` Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage and CPU usage.
- `health interval` Configures the sampling interval between health statistics checks.

**MIB Objects**

- HealthThreshInfo
  - `healthThreshDeviceRxLimit`
  - `healthThreshDeviceTxRxLimit`
  - `healthThreshDeviceMemoryLimit`
  - `healthThreshDeviceCpuLimit`
show health

Displays the health statistics for the switch. Statistics are displayed as percentages of total resource capacity and represent data taken from the last sampling interval.

**show health [port chassis/slot/port | slot chassis/slot[-slot2]] [statistics]**

---

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port**: To view a specific port, enter the slot and port number (3/1) along with the **port** keyword (port 3/1).
- **slot[-slot2]**: To view a series of slots, enter the range of slot numbers along with the **slot** keyword (1-10).
- **statistics**: Optional command syntax. It displays the same information as the **show health** command.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no slot or port information is specified, the aggregate health statistics for all ports is displayed.

**Examples**

```bash
-> show health
CMM Resources Current 1 Min 1 Hr 1 Day
-------------------+---------+-------+------+
CPU                0       0     0     0
Memory             30      30     24    24

-> show health port 1/1/24
Port 1/1/24 Resources Limit Current 1 Min 1 Hr 1 Day
-------------------+---------+-------+------+
Receive            80      01     01    01    01
Transmit/Receive   80      01     01    01    01
```

OmniSwitch AOS Release 8 CLI Reference Guide April 2023
Output definitions

- **Receive**: Traffic received by the switch.
- **Transmit/Receive**: Traffic transmitted and received by the switch.
- **Memory**: Switch memory.
- **CPU**: Switch CPU.
- **Limit**: Currently configured device threshold levels.
- **Curr**: Current device bandwidth usage.
- **1 Min Avg**: Average device bandwidth usage over a 1-minute period.
- **1 Hr Avg**: Average device bandwidth usage over a 1-hour period.
- **1 Hr Max**: Maximum device bandwidth usage over a 1-hour period (the maximum of the 1 minute averages).

Release History

Release 7.1.1; command introduced.
Release 8.5R1; **Limit** output field included.

Related Commands

- **show health all**: Displays health statistics for a specified resource on all NIs currently operating in the chassis.

MIB Objects

- **healthModuleTable**
  - **healthModuleSlot**
  - **healthModuleRxLatest**
  - **healthModuleRx1MinAvg**
  - **healthModuleRx1HrAvg**
  - **healthModuleRx1HrMax**
  - **healthModuleRxTxLatest**
  - **healthModuleRxTx1MinAvg**
  - **healthModuleRxTx1HrAvg**
  - **healthModuleRxTx1HrMax**
  - **healthModuleMemoryLatest**
  - **healthModuleMemory1MinAvg**
  - **healthModuleMemory1HrAvg**
  - **healthModuleMemory1HrMax**
  - **healthModuleCpuLatest**
  - **healthModuleCpu1MinAvg**
  - **healthModuleCpu1HrAvg**
  - **healthModuleCpu1HrMax**
show health all

Displays health statistics for a specified resource on all *active NI modules* installed in the chassis.

```
show health all {memory | cpu | rx | txrx}
```

**Syntax Definitions**

- **memory**: Displays the RAM memory health statistics for all active NI modules in the switch.
- **cpu**: Displays the CPU health statistics for all active NI modules.
- **rx**: Displays the health statistics for traffic *received* on all active NI modules.
- **txrx**: Displays the health statistics for traffic both *transmitted and received* on all active NI modules.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show health all memory
```

```
* - current value exceeds threshold
```

<table>
<thead>
<tr>
<th>Memory</th>
<th>1 Min</th>
<th>1 Hr</th>
<th>1 Hr</th>
<th>1 Hr</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Curr</td>
<td>Avg</td>
<td>Avg</td>
<td>Max</td>
</tr>
<tr>
<td>01</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>02</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>03</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>04</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>05</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>06</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>07</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>13</td>
<td>40</td>
<td>40</td>
<td>40</td>
<td>40</td>
</tr>
</tbody>
</table>
**Output Definitions**

<table>
<thead>
<tr>
<th>Memory (Cpu, TXRX, RX)</th>
<th>A list of all currently-active NI modules (i.e., active slots) on the switch. The column header corresponds with the resource keyword entered. For example, if <code>show health all cpu</code> is entered, <code>Cpu</code> is used as the column header.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curr</td>
<td>Current usage of the resource on the corresponding slot, in percent (the amount of the total resource bandwidth actually being used by the switch applications).</td>
</tr>
<tr>
<td>1 Min Avg</td>
<td>Average usage of the resource on the corresponding slot over a one minute period.</td>
</tr>
<tr>
<td>1 Hr Avg</td>
<td>Average usage of the resource on the corresponding slot over a one hour period.</td>
</tr>
<tr>
<td>1 Hr Max</td>
<td>The highest average hourly usage for the resource on the corresponding slot.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `show health` Displays the health statistics for the switch.
- `health threshold` Configures thresholds for input traffic (RX), output/input traffic (TX/RX), memory usage, and CPU usage.

**MIB Objects**

```
healthModuleTable
  healthModuleSlot
  healthModuleRxLatest
  healthModuleRx1MinAvg
  healthModuleRx1HrAvg
  healthModuleRx1HrMax
  healthModuleRxTxLatest
  healthModuleRxTx1MinAvg
  healthModuleRxTx1HrAvg
  healthModuleRxTx1HrMax
  healthModuleMemoryLatest
  healthModuleMemory1MinAvg
  healthModuleMemory1HrAvg
  healthModuleMemory1HrMax
  healthModuleCpuLatest
  healthModuleCpu1MinAvg
  healthModuleCpu1HrAvg
  healthModuleCpu1HrMax
```
Service provider networks are large and complex with a wide user base, and they often involve different operators that must work together in order to provide end-to-end services to enterprise customers. Operations, Administration, and Maintenance (OAM) provides service assurance over a converged network that service providers are looking for in an Ethernet network. Ethernet OAM addresses areas such as availability, mean time to repair and more. Ethernet OAM focuses on two main areas that are most in need by service providers and are rapidly evolving in the standards bodies, Service OAM and Link OAM. These two OAM protocols have unique objectives but are complementary to each other. Service OAM provides monitoring and troubleshooting of end-to-end Ethernet service instances, while Link OAM allows a provider to monitor and troubleshoot an individual Ethernet link.

MIB information for the Ethernet OAM commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Alcatel-IND1-ETHERNET-OAM-MIB.mib</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>alcatelIND1EoamMIB</td>
</tr>
<tr>
<td>Filename</td>
<td>IEEE8021-CFM-MIB.mib</td>
</tr>
<tr>
<td>Module</td>
<td>ieee8021CfmMib</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>EthOAM_vlan Configuration Commands</th>
<th>ethoam_vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>EthOAM Domain Configuration Commands</td>
<td>ethoam_domain</td>
</tr>
<tr>
<td>EthOAM Management Association Configuration Commands</td>
<td>ethoam_association</td>
</tr>
<tr>
<td>EthOAM Default-Domain Configuration Commands</td>
<td>ethoam_default-domain_level</td>
</tr>
</tbody>
</table>
| EthOAM Management Point Configuration Commands | ethoam endpoint  
|                                             | ethoam endpoint admin-state  
|                                             | ethoam endpoint rfp  
|                                             | ethoam endpoint ccm  
|                                             | ethoam endpoint priority  
|                                             | ethoam endpoint lowest-priority-defect  
|                                             | ethoam endpoint ctag-priority |
| EthOAM Loopback and Linktrace Commands      | ethoam linktrace  
|                                             | ethoam loopback |
| EthOAM Timer Configuration Commands         | ethoam fault-reset-time |
| EthOAM Performance Monitoring Configuration Commands | ethoam one-way-delay  
|                                             | ethoam two-way-delay  
|                                             | clear ethoam |
| EthOAM Show Commands                        | show ethoam  
|                                             | show ethoam domain  
|                                             | show ethoam domain association  
|                                             | show ethoam domain association end-point  
|                                             | show ethoam default-domain configuration  
|                                             | show ethoam default-domain  
|                                             | show ethoam remote-endpoint domain  
|                                             | show ethoam cfmstack  
|                                             | show ethoam linktrace-reply  
|                                             | show ethoam linktrace-tran-id  
|                                             | show ethoam vlan  
|                                             | show ethoam statistics  
|                                             | show ethoam config-error  
|                                             | show ethoam one-way-delay  
|                                             | show ethoam two-way-delay |
**ethoam vlan**

Creates an association between Primary VID and Non-Primary VID(s).

```
ethoam vlan vlanid_list primary-vlan vlan_id
```

```
no ethoam vlan vlanid_list
```

**Syntax Definitions**

- `vlanid_list` A list of VLAN Identifiers (e.g., ’10 30-40’ or ’10’).
- `vlan_id` VLAN Identifier (e.g., ’20’).

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Each VLAN ID specified must be created before creating any association.
- Each VLAN ID specified must be between 1 and 4094.
- Each VLAN ID specified must be static.
- A Non-Primary VID can only be associated with single Primary VID.
- Once Primary VID is associated with Non-Primary VID, then it can not be configured as Non-Primary VID. Its association must be removed before it is configured as Non-Primary VID.
- This CLI shall trigger Automip for this VLAN, if either ‘mhf’ is enabled for MA or default-MD with primary VLAN same as the primary VLAN of this VLAN.
- If the VLAN is deleted using VLAN CLI (no vlan vlan_id) and VLAN is non-primary, then the entry for this VLAN in the VLAN table will be deleted. This shall in turn delete all MEPs and MIPs associated with it. If the deleted VLAN is primary VLAN, then all its associated VLAN entries in the VLAN table shall be deleted. This shall in turn delete all MAs on this deleted VLAN.
- Use the no form of this command to dissociate Primary VID from the Non-Primary VID(s).

**Examples**

```
-> ethoam vlan 10 primary-vlan 20
```
-> ethoam vlan 11-15 primary-vlan 20
-> ethoam vlan 30 40-50 primary-vlan 20
-> no ethoam vlan 10

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **show ethoam vlan**
  Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge.

**MIB Objects**

dotlagCfmVlanTable
  dotlagCfmVlanComponentId
  dotlagCfmVlanVid
  dotlagCfmVlanPrimaryVid
  dotlagCfmVlanRowStatus
**ethoam domain**

Creates an Ethernet domain with a specific name.

```
ethoam domain md_name format {none | dnsname | mac-address-uint | string} level num
```

```
no ethoam domain name
```

### Syntax Definitions

- **md_name**
  - Specifies the domain name.
- **none**
  - This format is supported for the inter-op with ITU-T Y.1731.
- **dnsname**
  - Domain Name like string, globally unique text string derived from a DNS name.
- **mac-address-uint**
  - MAC address + 2-octet (unsigned) integer.
- **string**
  - Character String.
- **num**
  - MD Level and it ranges from 0 to 7.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Maximum domain length is 43.
- Use format as ‘none’ for inter-op with ITU-T Y.1731.
- Domain name is unique in a system.
- Deletion of MD shall result in the deletion of all MAs, MEPs, and MIPs configured in the MD.

### Examples

- `-> ethoam domain MD format none level 3`
- `-> ethoam domain MD1 format string level 4`

### Release History

Release 7.3.1; command was introduced.
Related Commands

show ethoam
Displays the information of all the Management Domains (MD) configured on the bridge.

show ethoam domain
Displays the information of a specific Management Domain configured on the bridge.

MIB Objects

dot1agCfmMdTable
  dot1agCfmMdName
  dot1agCfmMdFormat
  dot1agCfmMdLevel
**ethoam domain mhf**

Configure the Message Handling Function (MHF) value for MD entry.

```
ethoam domain md_name mhf {none | explicit | default}
```

### Syntax Definitions

- **md_name**: Specifies the domain name used while creating the management domain for which this management association is created.
- **none**: No MHFs can be created.
- **explicit**: MHFs can be created only if a MEP is created at some lower MD Level.
- **default**: MHFs can be created.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>explicit</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 X32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

Domain must be created before it is modified.

### Examples

```
-> ethoam domain MD mhf default
```

### Release History

Release 7.3.1; command was introduced.

### Related Commands

- **show ethoam**: Displays the information of all the Management Domains (MD) configured on the bridge.

### MIB Objects

- dotlagCfmMdTable
- dotlagCfmMdName
dotlagCfmMdMhfCreation
**ethoam domain id-permission**

Configures the ID-permission value for MD entry.

```
ethoam domain md_name id-permission {none | chassisid}
```

---

**Syntax Definitions**

- `md_name` Specifies the domain name used while creating the management domain for which this management association is created.
- `none` Sender ID TLV is not to be sent.
- `chassisid` Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present. System name shall be filled as Chassis ID.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>chassisid</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Domain must be created before it is modified.

---

**Examples**

```
-> ethoam domain MD id-permission chassisid
```

---

**Release History**

Release 7.3.1; command was introduced.
**Related Commands**

*show ethoam default-domain configuration*  
Displays the values of scalar Default-MD objects.

*show ethoam domain*  
Displays the information of a specific Management Domain configured on the bridge.

**MIB Objects**

dot1agCfmMdTable
  
dot1agCfmMdName
  
dot1agCfmMdIdPermission
**ethoam association**

Creates Maintenance Association (MA) entry.

```
ethoam association ma_name format {vpnid | unsignedint | string | primaryvid | icc-based} domain md_name
```

```
no ethoam association ma_name domain md_name
```

### Syntax Definitions

- **ma_name** Association name for the created Ethernet OAM Association.
- **vpnid** As specified in RFC 2685 VPN ID.
- **unsignedint** 2-octet unsigned integer.
- **string** Character String.
- **primaryvid** Primary VLAN ID (12 bits represented in a 2-octet integer).
- **icc-based** This format is supported for inter-op with ITU-T.
- **md_name** Specifies the domain name used while creating the management domain for which this management association is created.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Maximum association name is name 44 minus the length of its domain name.
- Use format as ‘icc-based’ to inter-op with ITU-T Y.1731.
- Domain must be created before the creation of MA.
- VLAN must be created before the creation of MA.
- VLAN specified must be a primary VID.
- Deletion of MA shall result in the deletion of MIPs and MEPs (on primary and non-primary VLAN) configured in it.
- Use the **no** form of the command to delete the Maintenance Association (MA) entry.
**Examples**

-> ethoam association MA format string domain MD
-> no ethoam association MA format string domain MD

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ethoam domain association</td>
<td>Displays the information of a specified MA in a Management Domain configured on the bridge.</td>
</tr>
</tbody>
</table>

**MIB Objects**

dotlagCfmMaNetTable
  dotlagCfmMaNetFormat
  dotlagCfmMaNetName
  dotlagCfmMaNetRowStatus

dotlagCfmMaCompTable
  dotlagCfmMaComponentId
  dotlagCfmMaCompPrimaryVid
  dotlagCfmMaCompRowStatus
ethoam association primary vlan

Creates a primary VLAN for the Maintenance Association (MA) entry.

```
ethoam association ma_name domain md_name primary-vlan vlan_id
no ethoam association ma_name domain md_name primary-vlan vlan_id
```

**Syntax Definitions**

- `ma_name` Association name for the created Ethernet OAM Association.
- `md_name` Specifies the domain name used while creating the management domain for which this management association is created.
- `vlan_id` Primary VLAN Identifier.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Domain must be created before the creation of MA.
- VLAN ID specified must be between 1 and 4094.
- Deletion of MA shall result in the deletion of MIPs and MEPs (on primary and non-primary VLAN) configured in it.
- Use the `no` form of the command to remove the Primary VLAN association.

**Examples**

```
-> ethoam association MA domain MD primary-vlan 100
-> no ethoam association MA domain MD primary-vlan 100
```

**Release History**

Release 7.3.1; command was introduced.
Related Commands

**show ethoam domain association**

Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

dot1agCfmMaCompTable

dot1agCfmMaComponentId
dot1agCfmMaCompPrimaryVid
dot1agCfmMaCompRowStatus
**ethoam association mhf**

Configures the MIP Half Function (MHF) value for MA Entry.

```
ethoam association ma_name domain md_name mhf {none | default | explicit | defer}
```

<table>
<thead>
<tr>
<th>Syntax Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ma_name</code></td>
</tr>
<tr>
<td><code>md_name</code></td>
</tr>
<tr>
<td><code>none</code></td>
</tr>
<tr>
<td><code>default</code></td>
</tr>
<tr>
<td><code>explicit</code></td>
</tr>
<tr>
<td><code>defer</code></td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>none</code></td>
<td>defer</td>
</tr>
<tr>
<td><code>explicit</code></td>
<td></td>
</tr>
<tr>
<td><code>default</code></td>
<td></td>
</tr>
<tr>
<td><code>defer</code></td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 C32E/T24C2/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- MA must be created before it is modified.
- On modification of ‘mhf’ for any MA, Automip shall also be invoked for all VLANS associated with this primary VID.

**Examples**

```
-> ethoam association MA domain MD mhf-creation defer
```

**Release History**

Release 7.3.1; command was introduced.
Related Commands

- `show ethoam domain association`  Displays the information of a specified MA in a Management Domain configured on the bridge.
- `show ethoam default-domain`  Displays the information of the default MA.

MIB Objects

- `dot1agCfmMaNetTable`
  - `dot1agCfmMaNetName`
- `dot1agCfmMaCompTable`
  - `dot1agCfmMaCompMhfCreation`
ethoam association id-permission

Configure id-permission value for MA Entry.

**ethoam association ma\_name domain md\_name id\_permission \{none | chassisid | defer\}**

### Syntax Definitions

- **ma\_name**: Association name for the created Ethernet OAM Association.
- **md\_name**: Specifies the domain name used while creating the management domain for which this management association is created.
- **none**: Sender ID TLV is not to be sent.
- **chassisid**: Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.
- **defer**: The contents of the Sender ID TLV are determined by the corresponding MD object ‘dot\_lag\_CfmMdIdPermission’.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>defer</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8</th>
<th>C32E/T24C2</th>
<th>X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

MA must be created before it is modified.

### Examples

- `-> ethoam association MA domain MD id-permission defer`

### Release History

Release 7.3.1; command was introduced.
**Related Commands**

- `show ethoam domain association` Displays the information of a specified MA in a Management Domain configured on the bridge.
- `show ethoam domain` Displays the information of a specific Management Domain configured on the bridge.

**MIB Objects**

- `dot1agCfmMaNetTable`
  - `dot1agCfmMaNetName`
- `dot1agCfmMaCompTable`
  - `dot1agCfmMaCompMIdPermission`
**ethoam association ccm-interval**

Modifies the Continuity Check Message (CCM) transmission interval of an Ethernet OAM Maintenance Association.

```
ethoam association ma_name domain {md_name | mac_address} ccm-interval {interval-invalid | interval100ms | interval1s | interval10s | interval1m | interval10m}
```

### Syntax Definitions

- **ma_name**: Name of the Ethernet OAM Association.
- **md_name**: Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain command on page 53-5.
- **mac_address**: Specifies the CFM system MAC address.
- **interval-invalid**: Specifies that no CCMs are sent by a MEP.
- **interval100ms**: Specifies the CCMs are sent every 100 milliseconds.
- **interval1s**: Specifies that CCMs are sent every 1 second.
- **interval10s**: Specifies that CCMs are sent every 10 seconds.
- **interval1m**: Specifies that CCMs are sent every minute.
- **interval10m**: Specifies that CCMs are sent every 10 minutes.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval-invalid</td>
<td>interval10s</td>
</tr>
<tr>
<td>interval100ms</td>
<td>interval1s</td>
</tr>
<tr>
<td>interval10s</td>
<td>interval1m</td>
</tr>
<tr>
<td>interval10m</td>
<td></td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>四肢末梢</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **ma_name** should be unique amid all those used by or available to the service provider within a domain.
Examples
-> ethoam association MA domain MD ccm-interval interval10s

Release History
Release 7.3.1; command was introduced.

Related Commands
show ethoam domain Displays the information of a specific Management Domain configured on the bridge.

MIB Objects
dot1agCfmMaNetTable
dot1agCfmMaNetName
dot1agCfmMaCompTable
dot1agCfmMaCompMIdPermission
ethoam association endpoint-list

Modifies the MEP list of an Ethernet OAM Maintenance Association.

```
ethoam association ma_name domain {md_name | mac_address} endpoint-list mep_id[-mep_id2]
no ethoam association ma_name domain {md_name | mac_address} endpoint-list mep_id[-mep_id2]
```

## Syntax Definitions

- **ma_name**: Name of the Ethernet OAM Association.
- **md_name**: Specifies the domain name. For more information on the different formats of the domain name, refer to the [ethoam domain command](page 53-5) on page 53-5.
- **mac_address**: Specifies the CFM system MAC address.
- **mep_id[-mep_id2]**: Specifies the MEP number. Use a hyphen to specify a range of MEP numbers.

## Defaults

N/A

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>No</td>
</tr>
</tbody>
</table>

## Usage Guidelines

- Use the **no** form of this command to remove the MEP list.
- Note that only the MEP that is associated with the MEP list of the MA can be configured locally on the bridge or monitored remotely.
- The **ma_name** should be unique within a domain.

## Examples

```
-> ethoam association MA domain MD endpoint-list 100-200
-> no ethoam association MA domain MD endpoint-list 100-200
```

## Release History

Release 7.3.1; command was introduced.
Related Commands

**show ethoam domain association**
Displays the information of a specified MA in a Management Domain configured on the bridge.

MIB Objects

dot1agCfmMdTable
dot1agCfmMdName
dot1agCfmMaNetTable
dot1agCfmMaNetName
DotlagCfmMaMepList
dot1agCfmMaMepListIdentifier
dot1agCfmMaMepListRowStatus
**ethoam association allowed-cvlan-list**

Configures allowed CVLANs on the Ethernet OAM Maintenance Association (MA).

```
ethoam association association_name domain {domain_name | mac_address} allowed-cvlan-list num[-num2]
```

```
no ethoam association association_name domain {domain_name | mac_address} allowed-cvlan-list num[-num2]
```

---

**Syntax Definitions**

- **association_name**
  - Name of the Ethernet OAM Association.

- **domain_name**
  - Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.

- **mac_address**
  - Specifies the CFM system MAC address.

- **num[-num2]**
  - Specifies the customer VLAN. Use hyphen to specify a range of VLANs.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `no` form of this command to remove the allowed CVLAN ID list from the MA.
- The CVLAN based maintenance endpoints can be created from CVLANs in the allowed CVLAN list.

---

**Examples**

```
-> ethoam association MA domain MD allowed-cvlan-list 10-15
```

```
-> no ethoam association MA domain MD allowed-cvlan-list 10-15
```

---

**Release History**

Release 8.8R1; command introduced.
**Related Commands**

- `show ethoam domain association` Displays the information of a specified MA in a Management Domain configured on the bridge.
- `ethoam endpoint` Creates a Maintenance End Point (MEP) and a virtual MEP.

**MIB Objects**

- `dotlagCfmMdTable`
  - `dotlagCfmMdName`
- `dotlagCfmMaNetTable`
  - `dotlagCfmMaNetName`
- `alaCfmMaCvlanListTable`
  - `alaCfmMaCvlanListIdentifier`
clear ethoam statistics

Clear statistics for all MEPs or for a particular MEP.

**clear ethoam statistics [domain md_name association ma_name endpoint mep_id]**

---

**Syntax Definitions**

- **ma_name**: Association name for the created Ethernet OAM Association.
- **md_name**: Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- **mep_id**: MEP Identifier. Valid Range is 1-8191.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Statistics are cleared for all MEPs if a specific MEP is not entered with this command.

---

**Examples**

- `-> clear ethoam statistics`
- `-> clear ethoam statistics domain MD association MA endpoint 10`

---

**Release History**

Release 7.3.1; command was introduced.
Related Commands

**show ethoam statistics**

Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

MIB Objects

dotlagCfmMdTable
  dotlagCfmMdName
dotlagCfmMaNetTable
  dotlagCfmMaNetName
dotlagCfmMepTable
  dotlagCfmMepIdentifier
  alaCfmMepClearStats
  alaCfmGlobalClearStats
**ethoam default-domain level**

Configure the effective level of all default domain entries with the level value set to no level.

`ethoam default-domain level num`

no ethoam default-domain

---

**Syntax Definitions**

`num` The MD level value. The valid range is 0-7.

**Defaults**

Default value is 0.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The MD level specified with this command applies to all default domain values that are currently set to no level.

**Examples**

`-> ethoam default-domain level 1`

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

`show ethoam default-domain configuration` Displays the values of scalar Default-MD objects.

**MIB Objects**

`DotlagCfmDefaultMdLevel`
**ethoam default-domain mhf**

Configure the effective MHF value for all default domain entries with MHF value set to **defer**.

```
ethoam default-domain mhf {none | default | explicit}
no ethoam default-domain
```

**Syntax Definitions**

- **none**: No MHFs can be created.
- **default**: MHFs can be created.
- **explicit**: MHFs can be created only if a MEP is created at some lower MD Level.

**Defaults**

Default value is **none**.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> ethoam default-domain mhf default
```

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show ethoam default-domain configuration`: Displays the values of scalar Default-MD objects.

**MIB Objects**

- `dotlagCfmDefaultMdDefMhfCreation`
**ethoam default-domain id-permission**

Configures the effective ID permission value for all default domain entries with the ID permission value set to `defer`.

`ethoam default-domain id-permission {none | chassisid}`

`no ethoam default-domain`

**Syntax Definitions**

`none`  
Sender ID TLV is not to be sent.

`chassisid`  
Chassis ID Length, Chassis ID Subtype and Chassis ID TLV are to be present.

**Defaults**

Default value is none.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> ethoam default-domain id-permission chassisid`

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

`show ethoam default-domain configuration`  
Displays the default domain configuration.

**MIB Objects**

`dot1agCfmDefaultMdDefIdPermission`
ethoam default-domain primary-vlan

Configures the default domain settings for the specified primary VLAN.

```
ethoam default-domain primary-vlan {vlan_id} [level {no-level | num}] [mhf {none | default | explicit | defer}] [id-permission {none | chassisid | defer}]
```

```
no ethoam default-domain
```

### Syntax Definitions

- **vlan_id**: VLAN Identifier.
- **no-level**: MD level is inherited from the default domain level.
- **num**: MD Level. Valid range is 0 to 7.
- **none**: No MHFs can be created.
- **default**: MHFs can be created.
- **explicit**: MHFs can be created only if a MEP is created at some lower MD Level.
- **defer**: MHF defers to the default domain MHF value.
- **none**: Sender ID TLV is not to be sent.
- **chassisid**: Chassis ID Length, Chassis ID Subtype, and Chassis ID TLV are to be present.
- **defer**: ID permission defers to the default domain ID permission value.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-level</td>
<td>num</td>
</tr>
<tr>
<td>no-level</td>
<td>no-level</td>
</tr>
<tr>
<td>none</td>
<td>explicit</td>
</tr>
<tr>
<td>defer</td>
<td>defer</td>
</tr>
<tr>
<td>none</td>
<td>chassisid</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

On modification of MHF for any primary VID, Automip is invoked for all VLANs associated with this primary VID.
Examples

-> ethoam default-domain primary-vlan 10 id-permission chassid level 3 mhf default.
-> ethoam default-domain primary-vlan 10 id-permission chassid
-> ethoam default-domain primary-vlan 10 level 3
-> ethoam default-domain primary-vlan 10 mhf default
-> ethoam default-domain primary-vlan 10 level 3 mhf default

Release History

Release 7.3.1; command was introduced..

Related Commands

show ethoam default-domain  Displays the information of all the default MD.

MIB Objects

dotlagCfmDefaultMdTable
   dotlagCfmDefaultMdComponentId
dotlagCfmDefaultMdPrimaryVid
dotlagCfmDefaultMdLevel
**ethoam endpoint**

Creates a Maintenance End Point (MEP) and virtual MEP.

```
ethoam endpoint mep_id domain md_name association ma_name direction {up | down} {port chassis/slot/port | virtual | linkagg agg_id} [primary-vlan vlan_id | cvlan cvlan_id]
```

```
no ethoam endpoint mep_id domain md_name association ma_name
```

**Syntax Definitions**

- `mep_id`: Specifies the Maintenance Association End Point. The range is 1–8191.
- `md_name`: Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- `ma_name`: Association name for the created Ethernet OAM Association.
- `up`: For UP MEP.
- `down`: For DOWN MEP.
- `chassis`: The chassis identifier.
- `slot/port`: Physical slot and port number on which MEP needs to be created.
- `virtual`: Keyword for creating virtual MEP.
- `agg_id`: Linkagg Identifier on which MEP needs to be created.
- `vlan_id`: VLAN Identifier.
- `cvlan_id`: Specifies the customer VLAN of the MEP. *This parameter is supported only on the OmniSwitch 6465 and OmniSwitch 6865.*

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete a maintenance endpoint.
- The `mep_id` must be unique amid all those used by or available to the service provider in the specified MA.
- The direction for virtual MEP must always be up.
For creating a virtual MEP the value of port must be given the keyword “virtual”.

- The CVLAN must be part of the allowed CVLAN list.
- The direction of CVLAN based MEP must always be configured as ‘UP’.
- The CVLAN based MEP must be configured on the UNI port.
- The CVLAN ID must be associated to the SVLAN (MA VLAN) and the UNI port using Ethernet service configuration.
- The SAP profile of the SVLAN (MA VLAN), CVLAN, and UNI port must be in ‘tag preserve’ mode.
- The removal of SAP, UNI port from SAP, CVLAN from the SAP, or changing the SAP profile to ‘tag translate mode’ removes the corresponding CVLAN based MEPS automatically.

**Examples**

-> ethoam endpoint 10 domain MD association MA direction up port 1/1/1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1
-> ethoam endpoint 10 domain MD association MA direction down linkagg 1 vlan 10
-> ethoam endpoint 1 domain md1 association ma1 direction up port virtual primary-vlan 100
-> ethoam endpoint 1 domain md1 association ma1 direction up port virtual primary-vlan 20
-> no ethoam endpoint 10 domain MD association MA

**Release History**

Release 7.3.1; command was introduced.
Release 8.8R1; cvlan parameter added.

**Related Commands**

- show ethoam domain association end-point
  Displays the information of a specific MEP in a Management Domain configured on the bridge.

**MIB Objects**

- dotlagCfmMdTable
  - dotlagCfmMdName
- dotlagCfmMaNetTable
  - dotlagCfmMaNetName
- dotlagCfmMepTable
  - dotlagCfmMepIdentifier
  - dotlagCfmMepDirection
  - dotlagCfmMepIfIndex
  - dotlagCfmMepPrimaryVid
- aLaCfmMepTable
  - alacfmMepCvlanId
ethoam endpoint admin-state

Configures the administrative state of MEP.

```
ethoam endpoint mep_id domain {md_name | mac_address} association ma_name admin-state {enable | disable}
```

**Syntax Definitions**

- `mep_id` Specifies the Maintenance Association End Point. The range is 1–8191.
- `md_name` Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- `mac_address` Specifies the CFM system MAC address.
- `ma_name` Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
- `enable` Administratively enables MEP.
- `disable` Administratively disables MEP.

**Defaults**

The default value is disable.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `mep_id` specified must already exist in the switch configuration.

**Examples**

```
-> ethoam endpoint 100 domain MD association MA admin-state enable
```

**Release History**

Release 7.3.1; command was introduced.
Related Commands

*show ethoam domain association end-point* 
Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

Dot1agCfmMep
  dot1agCfmMepIndex
  dot1agCfmMepIdentifier
  dot1agCfmMepDirection
  dot1agCfmMepPortNumber
  dot1agCfmMepMacAddress
  dot1agCfmMepAdminStatus
  dot1agCfmMepFngState
  dot1agCfmMepCcmEnabled
  dot1agCfmMepCcmTransmitting
  dot1agCfmMepCcmLtmPriority
  dot1agCfmMepCcmNotReceived
  dot1agCfmMepCcmStreamError
  dot1agCfmMepCcmStreamOther
  dot1agCfmMepRdiReceived
  dot1agCfmMepLastCcmMaFault
  dot1agCfmMepLastCcmCrossConnFault
  dot1agCfmMepCcmOut
  dot1agCfmMepLbmNextSeqNumber
  dot1agCfmMepLbrIn
  dot1agCfmMepLbrInOutOfOrder
  dot1agCfmMepLbrOut
  dot1agCfmMepLtmNextSeqNumber
  dot1agCfmMepLtmIn
  dot1agCfmMepLtmOut
  dot1agCfmMepDefectsPresent
  dot1agCfmMepDefectsAbsent
  dot1agCfmMepRowStatus
ethoam endpoint rfp

Enables or disables the Remote Fault Propagation (RFP) on MEP.

ethoam endpoint mep_id domain {md_name | mac_address} association ma_name rfp {enable | disable}

Syntax Definitions

mep_id Specifies the Maintenance Association End Point. The range is 1–8191.
md_name Specifies the domain name. For more information on the different formats of the domain name, refer to ethoam domain.
mac_address Specifies the CFM system MAC address.
ma_name Association name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
enable Administratively enables RFP on MEP.
disable Administratively disables RFP on MEP.

Defaults

The default value of RFP is disable.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The mep_id specified must already exist in the switch configuration.
- The domain and association must be created before RFP can be enabled.
- The MEP must be an UP MEP. If down MEP is specified, CLI returns with an error.
- The admin state of the MEP must be enabled in order to report faults.
- RFP cannot be enabled on virtual UP MEP since it is not associated with a physical interface.
- It is recommended that if RFP is enabled on a port, then any other violation feature (Link Monitoring or Link Fault Propagation) should not be configured.
- It is recommended that if RFP is enabled on a port, then automatic recovery is disabled for that port.
- If Link Monitoring is configured on a RFP enabled port, then the wait-to-restore timer must be less than the CCM interval.
**Examples**

`-> ethoam endpoint 1 domain md1 association ma1 rfp enable`
`-> ethoam endpoint 1 domain md1 association ma1 rfp disable`

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ethoam domain</code></td>
<td>Displays the information of a specific MEP in a Management Domain configured on the bridge.</td>
</tr>
<tr>
<td><code>association end-point</code></td>
<td></td>
</tr>
</tbody>
</table>

**MIB Objects**

- `Dot1agCfmMDTable`
  - `dot1agCfmMdName`
- `Dot1agCfmMaNetTable`
  - `dot1agCfmMaNetName`
- `Dot1agCfmMepTable`
  - `dot1agCfmMepIdentifier`
  - `dot1agCfmRfpEnabled`
ethoam endpoint ccm

Configures the MEP to generate Continuity Check Messages (CCM).

`ethoam endpoint mep_id domain {md_name | mac_address} association ma_name ccm {enable | disable}`

**Syntax Definitions**

- **mep_id**
  - Specifies the Maintenance Association End Point. The range is 1–8191.

- **md_name**
  - Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.

- **mac_address**
  - Specifies the CFM system MAC address.

- **ma_name**
  - Name of the Ethernet OAM association. Up to 48 (minus the domain name length) characters may be used.

- **enable**
  - Enables MEP to generate CCMs.

- **disable**
  - Disables MEP to generate CCMs.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `mep_id` should be unique amid all those used by or available to the service provider in the specified MA.

**Examples**

`-> ethoam endpoint 100 domain MD association MA ccm enable`

**Release History**

Release 7.3.1; command was introduced.
Related Commands

show ethoam domain association end-point

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

Dot1agCfmMep
  dot1agCfmMepIndex
  dot1agCfmMepIdenfier
  dot1agCfmMepDirection
  dot1agCfmMepPortNumber
  dot1agCfmMepMacAddress
  dot1agCfmMepAdminStatus
  dot1agCfmMepFngState
  dot1agCfmMepCcmEnabled
  dot1agCfmMepCcmTransmitting
  dot1agCfmMepCcmLtmPriority
  dot1agCfmMepCcmNotReceived
  dot1agCfmMepCcmStreamError
  dot1agCfmMepCcmStreamOther
  dot1agCfmMepRdiReceived
  dot1agCfmMepLastCcmMaFault
  dot1agCfmMepLastCcmCrossConnFault
  dot1agCfmMepCcmOut
  dot1agCfmMepLbmNextSeqNumber
  dot1agCfmMepLbrIn
  dot1agCfmMepLbrInOutOfOrder
  dot1agCfmMepLbrOut
  dot1agCfmMepLtmNextSeqNumber
  dot1agCfmMepLtmIn
  dot1agCfmMepLtmOut
  dot1agCfmMepDefectsPresent
  dot1agCfmMepDefectsAbsent
  dot1agCfmMepRowStatus
**ethoam endpoint priority**

Configures the priority values for CCMs and Linktrace Messages (LTMs) transmitted by a MEP.

```
ethoam endpoint mep_id domain {md_name | mac_address} association ma_name priority ccm_ltm_priority
```

### Syntax Definitions

- **mep_id** Specifies the Maintenance Association End Point. The valid range is 1–8191.

- **md_name** Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.

- **mac_address** Specifies the CFM system MAC address.

- **ma_name** Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

- **ccm_ltm_priority** Priority value for CCMs and LTMs transmitted by the MEP. The valid range is 0–7.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ccm_ltm_priority</td>
<td>7</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platforms</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **mep_id** should be unique amid all those used by or available to the service provider in the specified MA.

### Examples

```
-> ethoam endpoint 100 domain MD association MA priority 6
```

### Release History

Release 7.3.1; command was introduced.
Related Commands

```
show ethoam domain association end-point
```

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

```
DotlagCfmMep
    dotlagCfmMepIndex
dotlagCfmMepIdentifier
dotlagCfmMepDirection
dotlagCfmMepPortNumber
dotlagCfmMepMacAddress
dotlagCfmMepAdminStatus
dotlagCfmMepFngState
dotlagCfmMepCcmEnabled
dotlagCfmMepCcmTransmitting
dotlagCfmMepCcmLtmPriority
dotlagCfmMepCcmNotReceived
dotlagCfmMepCcmStreamError
dotlagCfmMepCcmStreamOther
dotlagCfmMepRdiReceived
dotlagCfmMepLastCcmMaFault
dotlagCfmMepLastCcmCrossConnFault
dotlagCfmMepCcmOut
dotlagCfmMepLbmNextSeqNumber
dotlagCfmMepLbrIn
dotlagCfmMepLbrInOutOfOrder
dotlagCfmMepLbrOut
dotlagCfmMepLtmNextSeqNumber
dotlagCfmMepLtmIn
dotlagCfmMepLtmOut
dotlagCfmMepDefectsPresent
dotlagCfmMepDefectsAbsent
dotlagCfmMepRowStatus
```
**ethoam endpoint lowest-priority-defect**

Configures the lowest priority fault alarm for the lowest priority defect for a MEP.

```
ethoam endpoint mep_id domain {md_name | mac_address} association ma_name lowest-priority-defect lowest_priority_defect
```

**Syntax Definitions**

- **mep_id**: Specifies the Maintenance Association End Point. The range is 1–8191.
- **md_name**: Specifies the domain name. For more information on the different formats of the domain name, refer to **ethoam domain**.
- **mac_address**: Specifies the CFM system MAC address.
- **ma_name**: Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
- **lowest_priority_defect**: The lowest priority defect that can generate a Fault alarm. Possible values are `xcon`, `rem-err-xcon`, `no-defect`, `mac-rem-err-xcon`, `err-xcon`, and `all-defect`.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>lowest_priority_defect</td>
<td>mac-rem-err-xcon</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **mep_id** should be unique amid all those used by or available to the service provider in the specified MA.

**Examples**

```
-> ethoam endpoint 100 domain esd.ale.com association ale-sales lowest-priority-defect all-defect
```

**Release History**

Release 7.3.1; command was introduced.
Related Commands

show ethoam domain association end-point

Displays the information of a specific MEP in a Management Domain configured on the bridge.

MIB Objects

DotlagCfmMep
  dotlagCfmMepIndex
  dotlagCfmMepIdentifier
  dotlagCfmMepDirection
  dotlagCfmMepPortNumber
  dotlagCfmMepMacAddress
  dotlagCfmMepAdminStatus
  dotlagCfmMepFngState
  dotlagCfmMepCcmEnabled
  dotlagCfmMepCcmTransmitting
  dotlagCfmMepCcmLtmPriority
  dotlagCfmMepCcmNotReceived
  dotlagCfmMepCcmStreamError
  dotlagCfmMepCcmStreamOther
  dotlagCfmMepRdiReceived
  dotlagCfmMepLastCcmMaFault
  dotlagCfmMepLastCcmCrossConnFault
  dotlagCfmMepCcmOut
  dotlagCfmMepLbmNextSeqNumber
  dotlagCfmMepLbrIn
  dotlagCfmMepLbrInOutOfOrder
  dotlagCfmMepLbrOut
  dotlagCfmMepLtmNextSeqNumber
  dotlagCfmMepLtmIn
  dotlagCfmMepLtmOut
  dotlagCfmMepDefectsPresent
  dotlagCfmMepDefectsAbsent
  dotlagCfmMepRowStatus
**ethoam endpoint ctag-priority**

Configures the priority value to be included in the inner tag of the CFM frames originating from CVLAN MEPs.

```
ethoam endpoint mep-id domain md-name association ma-name ctag-priority \{copy-outer-to-inner | num\}
```

### Syntax Definitions

- **mep_id**
  - Specifies the Maintenance Association End Point. The valid range is 1–8191.

- **ma-name**
  - Association name for the created Ethernet OAM Association.

- **md-name**
  - Specifies the domain name used while creating the management domain for which this management association is created.

- **copy-outer-to-inner**
  - Copies the outer tag priority to the inner tag.

- **num**
  - Specify an inner tag priority value. Valid range is 0 to 7.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy-outer-to-inner</td>
<td>copy-outer-to-inner</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

- If the priority value is not configured, by default, the outer tag priority value is considered as the inner-tag priority.

- The outer tag is the primary SVLAN of the MA and the inner tag is the CVLAN configured in the endpoint.

### Examples

```
-> ethoam endpoint 1 domain md1 association ma1 ctag-priority 6
-> ethoam endpoint 1 domain md1 association ma1 ctag-priority copy-outer-to-inner
```
**Release History**

Release 8.8R1; command introduced.

**Related Commands**

- **ethoam endpoint priority**
  - Configures the priority values for CCMs and Linktrace Messages (LTMs) transmitted by a MEP.

- **show ethoam domain association end-point**
  - Displays the information of a specific MEP in a Management Domain configured on the bridge.

**MIB Objects**

- `dotlagCfmMdTable`
  - `dotlagCfmMdName`
- `dotlagCfmMaNetTable`
  - `dotlagCfmMaNetName`
- `dotlagCfmMepTable`
  - `dotlagCfmMepIdentifier`
- `alaCfmMepTable`
  - `alaCfmMepCtagPriority`
  - `alaCfmMepCtagSet`
ethoam linktrace

Enables the maintenance entity to initiate transmitting Link Trace Messages (LTM).

```
ethoam linktrace {target-macaddress mac_address | target-endpoint t_mepid} source-endpoint s_mepid domain {md_name | mac_address} association ma_name [flag [fdb-mpdb | fdbonly]] [hop-count hop_count]
```

**Syntax Definitions**

- `mac_address`: Target MAC address to be transmitted.
- `t_mepid`: Specifies the MEP for which the Loopback message is targeted.
- `s_mepid`: Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
- `md_name`: Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- `domain mac_address`: Specifies the CFM system MAC address.
- `ma_name`: Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
- `fdbonly`: Specifies that only the MAC addresses learned in a bridge's active data forwarding table will be used to decide the egress port.
- `hop_count`: Indicates the number of hops remaining in this LTM. Each bridge that handles the LTM decreases the value by 1. This decreased value is returned to the LTM. The valid range is 1–2^32.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>flag</td>
<td>fdbonly</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command allows an operator to generate a LTM for the specified MEP.
- This command signals the MEP that it should transmit a Linktrace message and detect the presence or lack of the corresponding Linktrace messages.
**Examples**

-> ethoam linktrace target-macaddress 10:aa:ac:12:12:ad source 4 domain MD association flag fdbonly hop-count 32 Transaction Id: 6943

-> ethoam linktrace target-endpoint 15 source 4 domain MD association Transaction Id: 6934

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

*show ethoam domain* Displays the information of a specified Management Domain configured on the bridge.

**MIB Objects**

Dot1agCfmMep

- dot1agCfmMepIdentifier
- dot1agCfmMepTransmitLtmFlags
- dot1agCfmMepTransmitLtmTargetMacAddress
- dot1agCfmMepTransmitLtmTargetMepId
- dot1agCfmMepTransmitLtmTargetIsMepId
- dot1agCfmMepTransmitLtmTtl
- dot1agCfmMepTransmitLtmResult
- dot1agCfmMepTransmitEgressIdentifier
ethoam loopback

Initiates the transmission of loopback messages from the specified source MEP to the specified target MEP or MAC address. Also triggers the source MEP to detect the presence or lack of a corresponding loopback reply from the target.

```
ethoam loopback \{target-endpoint t_mepid | target-macaddress mac_address\} source-endpoint s_mepid domain md_name association ma_name [number num] [data string] [vlan-priority vlan_priority] [drop-eligible \{true | false\}]
```

Syntax Definitions

- **t_mepid**: Specifies the MEP for which the Loopback message is targeted. The valid range is 1-8191.
- **mac_address**: Target MAC address to be transmitted.
- **s_mepid**: Specifies the MEP that transmits the Loopback message. The valid range is 1–8191.
- **md_name**: Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- **ma_name**: Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
- **num**: Number of loopback messages. The valid range is 1-10.
- **string**: Specifies the amount of data to be included in the Data Type Length Value (TLV), if the Data TLV is selected to be sent. The valid range is 1–255.
- **vlan_priority**: VLAN Priority. The valid range is 0-7.
- **true**: Sets the drop eligibility bit in the VLAN tag to true.
- **false**: Sets the drop eligibility bit in the VLAN tag to false.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>1</td>
</tr>
<tr>
<td>vlan_priority</td>
<td>CCM priority</td>
</tr>
<tr>
<td>drop-eligible</td>
<td>true</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Usage Guidelines

- Source and target MEP-ID, MD and MA must already exist before loopback is initiated.
- If data TLV is not set, then it is not sent in the loopback message.

Examples

-> ethoam loopback target-endpoint 10 source-endpoint 20 domain MD association MA number 3
Reply from 00:0E:B1:6B:43:89: bytes=64 seq=0 time=100ms
Reply form 00:0E:B1:6B:43:89: bytes=64 seq=0 time=112ms
Request timed out.
----00:E0:B1:6B:43:89 ETH-LB Statistics----
3 packets transmitted, 2 packets received, 33% packet loss
round-trip (ms) min/avg/max = 100/106/112

Release History

Release 7.3.1; command was introduced.

Related Commands

show ethoam domain Displays the information of a specified Management Domain configured on the bridge.

MIB Objects

dotlagCfmMdTable
dotlagCfmMdName
dotlagCfmMaNetTable
dotlagCfmMaNetName
dotlagCfmMepTable
dotlagCfmMepIdentifier
dotlagCfmMepTransmitLbmDestMacAddress
dotlagCfmMepTransmitLbmDestMepId
dotlagCfmMepTransmitLbmDestIsMepId
dotlagCfmMepTransmitLbmMessages
dotlagCfmMepTransmitLbmDataTlv
dotlagCfmMepTransmitLbmVlanPriority
dotlagCfmMepTransmitLbmVlanDropEnable
dotlagCfmMepTransmitLbmStatus
**ethoam fault-alarm-time**

Configures the timeout value for the Fault Notification Generation Alarm time that specifies the time interval during which one or more defects should be detected before the fault alarm is issued.

```
ethoam fault-alarm-time centiseconds endpoint mep_id domain md_name association ma_name

no ethoam fault-alarm-time endpoint mep_id domain md_name association ma_name
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>centiseconds</code></td>
<td>The Fault Notification Generation Alarm timeout value, in centiseconds. The valid range is 250–1000.</td>
</tr>
<tr>
<td><code>mep_id</code></td>
<td>Specifies the MEP of a specific MA. The valid range is 1–8191.</td>
</tr>
<tr>
<td><code>md_name</code></td>
<td>Specifies the domain name. For more information on the different formats of the domain name, refer to <code>ethoam domain</code>.</td>
</tr>
<tr>
<td><code>ma_name</code></td>
<td>Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>centiseconds</code></td>
<td>250</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to restore the Fault Notification Generation Alarm timeout value to the default value.
- The Fault Notification Generation Alarm timeout value is configurable per MEP.

**Examples**

```
-> ethoam fault-alarm-time 500 endpoint 100 domain esd.ale.com association ale_sales
-> no ethoam fault-alarm-time endpoint 100 domain esd.ale.com association ale_sales
```
**Release History**
Release 7.3.1; command was introduced.

**Related Commands**
- `show ethoam domain association end-point` Displays the information of a specific MEP in a Management Domain configured on the bridge.

**MIB Objects**
- `Dot1agCfmMep`
  - `dot1agCfmMepFngAlarmTime`
**ethoam fault-reset-time**

Configures the timer value for the Fault Notification Generation Reset time that specifies the time interval during which the fault alarm is re-enabled to process faults. The fault alarm will only be re-enabled if no new faults are received during this time interval.

```
ethoam fault-reset-time centiseconds endpoint mep_id domain md_name association ma_name
no ethoam fault-reset-time endpoint mep_id domain md_name association ma_name
```

### Syntax Definitions

- **centiseconds**
  - The Fault Notification Generation Reset timer value, in centi seconds. The valid range is 250–1000.
- **mep_id**
  - Specifies the MEP of a specific MA. The valid range is 1–8191.
- **md_name**
  - Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- **ma_name**
  - Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>centiseconds</td>
<td>1000</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `no` form of this command to restore the Fault Notification Generation Reset timeout value to the default value.
- The Fault Notification Generation Reset timer value is configurable per MEP.

### Examples

```
-> ethoam fault-reset-time 250 end-point 100 domain esd.ale.com association ale_sales
-> no ethoam fault-reset-time end-point 100 domain esd.ale.com association ale_sales
```
**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **ethoam fault-alarm-time**
  
  Configures the timeout value for the Fault Notification Generation Alarm time.

- **show ethoam domain association end-point**
  
  Displays the information of a specific MEP in a Management Domain configured on the bridge.

**MIB Objects**

- **DotlagCfmMep**
  
  - **dotlagCfmMepFngResetTime**
**ethoam one-way-delay**

Initiates a one-way-delay measurement (1DM) to determine the one-way frame delay (latency) and delay variation (jitter) between two MEPs.

`ethoam one-way-delay {target-endpoint t_mepid | target-macaddress mac_address} source-endpoint s_mepid domain md_name association ma_name [vlan- priority vlan_priority]`

**Syntax Definitions**

- **t_mepid**: Target MEP ID. The valid range is 1-8191.
- **mac_address**: Target MAC address.
- **s_mepid**: Source MEP ID. The valid range is 1–8191.
- **md_name**: Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- **ma_name**: Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
- **vlan_priority**: VLAN Priority. The valid range is 0-7.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_priority</td>
<td>7</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Source MEP-ID, MD and MA must be created before initiating 1DM.

- When `target-endpoint` is specified then entry must be present in the RMEP table, no matter if its status is RMEP_OK or RMEP_FAILED, before initiating 1DM. So `target-macaddress` can be used to bypass such a restriction.

- Although the OmniSwitch implementation of Ethernet frame delay measurement (ETH-DM) is compliant with ITU-T Y.1731, delay measurement can be performed for both ITU-T Y.1731 and IEEE 802.1ag MEPs.

- If the 1DM is initiated with a `target-macaddress` and an egress port is found for this MAC address, then the 1DM frames are transmitted from that port. Otherwise, 1DM frames are flooded in the MEP’s VLAN.
• One-way delay measurement requires NTP clock synchronization between the sending and receiving MEPs.

**Examples**

```plaintext
-> ethoam one-way-delay target-endpoint 10 source-endpoint 12 domain MD association MA vlan-priority 4
-> ethoam one-way-delay target-macaddress 00:e0:bl:6a:52:4c source-endpoint 12 domain MD association MA vlan-priority 4
```

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show ethoam one-way-delay`  Displays the one-way-delay and jitter parameters for all entries or for the MAC address of a specific MEP.

**MIB Objects**

- `dot1agCfmMdTable`
  - `dot1agCfmMdName`
- `dot1agCfmMaNetTable`
  - `dot1agCfmMaNetName`
- `dot1agCfmMepTable`
  - `dot1agCfmMepIdentifier`
- `alaCfmMepTable`
  - `alaCfmMepOWDTMacAddress`
  - `alaCfmMepOWDTMepIdentifier`
  - `alaCfmMepOWDTPriority`
**ethoam two-way-delay**

Initiate a two-way-delay measurement to determine the round-trip latency and jitter between two MEPs. The initiating MEP sends delay measurement message (DMM) frames to the receiving MEP. The receiving MEP responds with delay measurement reply (DMR) frames.

```
ethoam two-way-delay {target-endpoint t_mepid | target-macaddress mac_address} source-endpoint s_mepid domain md_name association ma_name [vlan-priority vlan_priority]
```

**Syntax Definitions**

- **t_mepid**: Target MEP ID. The valid range is 1-8191.
- **mac_address**: Target MAC address.
- **s_mepid**: Source MEP ID. The valid range is 1–8191.
- **md_name**: Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.
- **ma_name**: Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
- **vlan_priority**: VLAN Priority. The valid range is 0-7.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_priority</td>
<td>7</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Source MEP-ID, MD and MA must be created before initiating a two-way delay measurement.
- When `target-endpoint` is specified then entry must be present in the RMEP table, no matter if the status is RMEP_OK or RMEP_FAILED, before initiating two-way-delay. So `target-macaddress` can be used to bypass such a restriction.
- The CLI console will pause until all DMRs are received or maximum of 3 seconds to ensure that all the DMRs have been returned. If the operation fails, then the appropriate message is displayed. If the operation is successful, no message is displayed.
- If the DMM is initiated by UP MEP with a target-macaddress and the egress port is found for this MAC address, then DMM frames are transmitted from that port. Otherwise, DMM frames are flooded in the MEP’s VLAN.

- Two-way delay measurement does not require NTP clock synchronization on the sending and receiving MEPs.

- Although the OmniSwitch implementation of Ethernet frame delay measurement (ETH-DM) is compliant with ITU-T Y.1731, delay measurement can be performed for both ITU-T Y.1731 and IEEE 802.1ag MEPs.

- This command initiates an on-demand OAM performance measurement. To set up continuous two-way delay measurement, see the “Service Assurance Agent Commands” chapter for information about how to configure an SAA for continuous two-way frame delay measurement.

**Examples**

```
-> ethoam two-way-delay target-endpoint 10 source-endpoint 12 domain MD association MA vlan-priority 4
Reply from 00:0E:B1:6B:43:89 delay=2584us jitter=282us
-> ethoam two-way-delay target-macaddress 00:e0:b1:6a:52:4c source-endpoint 12
domain MD association MA vlan-priority 4
Reply from 00:E0:B1:6A:52:4C: delay=2584us jitter=282us
```

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

`show ethoam two-way-delay` Displays the two-way-delay delay and jitter parameters for all entries or for the MAC address of a specific MEP.

**MIB Objects**

- `dot1agCfmMdTable`
- `dot1agCfmMdName`
- `dot1agCfmMaNetTable`
- `dot1agCfmMaNetName`
- `dot1agCfmMepTable`
- `dot1agCfmMepIdentifier`
- `alaCfmMepTable`
- `alaCfmMepTWDTMacAddress`
- `alaCfmMepTWDTMepIdentifier`
- `alaCfmMepTWDTPriority`
**clear ethoam**

Delete all the one-way-delay or two-way-delay entries.

```
clear ethoam {one-way-delay-table | two-way-delay-table}
```

### Syntax Definitions

**one-way-delay-table**
Clears the one-way delay measurement table.

**two-way-delay-table**
Clears the two-way delay measurement table.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> clear ethoam one-way-delay-table
-> clear ethoam two-way-delay-table
```

### Release History

Release 7.3.1; command was introduced.

### Related Commands

**ethoam one-way-delay**
Initiates the two one-way-delay messages from a particular MEP to an RMEP.

### MIB Objects

- alaCfmGlobalOWDClear
- alaCfmGlobalTWDClear
**show ethoam**

Displays the information of all the Management Domains (MD) configured on the bridge.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays all the MAs for all the MDs.

**Examples**

-> show ethoam
System Configuration
    Ethernet OAM system mac address: 00:D0:95:EC:84:B0,
    Number of Maintenance Domains: 1
    Maintenance Domain: esd.ale.com
    Maintenance Association: ale-sales

**output definitions**

- **Ethernet OAM system mac address**: The MAC address of the Ethernet OAM system.
- **Number of Maintenance Domains**: The number of maintenance domains configured on the bridge.
- **Maintenance Domain**: The name of the maintenance domain.
- **Maintenance Association**: The name of the maintenance association.

**Release History**

Release 7.3.1; command was introduced.
**Related Commands**

*ethoam domain*  
Creates an Ethernet domain with a specific name.

**MIB Objects**

Dot1agCfmMd
- dot1agCfmMdName

Dot1agCfmMa
- dot1agCfmMaName
show ethoam domain

Displays the information of a specific Management Domain configured on the bridge.

show ethoam domain md_name

Syntax Definitions

*md_name*  
Specifies the management domain name.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ethoam domain MD
Total number of MAs configured in this MD = 1
MD Attributes
  MD-Format : string,
  MD-Level : level-3,
  MD-MHFstatus : mhfNone,
  MD-IdPermission : sendIdNone
  Maintenance Association : MA
    MA-Format : string,
    Primary Vlan : 199,
    Associated Vlan-list : none,
    Total Number of Vlans : 1,
    MA-MHFstatus : mhfNone,
    MA-IdPermission : sendIdNone,
    CCM-interval : interval10s,
    MEP-List(MEP-Id) : 10
    CVLAN-List(CVLAN-Id) : 200

output definitions

<table>
<thead>
<tr>
<th>MD-level</th>
<th>The level at which the MD was created.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD-MHFstatus</td>
<td>Indicates whether the maintenance entity can create MHFs for this MD. Options include none, explicit, or default.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Maintenance Association</th>
<th>The name of the maintenance association.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan</td>
<td>The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.</td>
</tr>
<tr>
<td>MA-MHFstatus</td>
<td>Indicates whether the maintenance entity can create MHFs for this MA. Options include none, explicit, or default.</td>
</tr>
<tr>
<td>CCM-interval</td>
<td>The interval between the CCM transmissions.</td>
</tr>
<tr>
<td>MEP-Id</td>
<td>Indicates the Maintenance End Point.</td>
</tr>
<tr>
<td>CVLAN-List(CVLAN-Id)</td>
<td>The CVLAN configured for the MEPs in a MA.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.
Release 8.8R1; CVLAN-List (CVLAN-Id) field added in the output.

Related Commands

- **show ethoam**
  Displays the information of all the Management Domains (MD) configured on the bridge.

- **ethoam domain**
  Creates an Ethernet domain with a specific name.

MIB Objects

- `DotlagCfmMd`
  - `dotlagCfmMdLevel`
  - `dotlagCfmMdMhfCreation`

- `DotlagCfmMa`
  - `dotlagCfmMaName`
  - `dotlagCfmMaVid`
  - `dotlagCfmMaMhfCreation`
  - `dotlagCfmMaCcmInterval`
  - `DotlagCfmMep`
  - `dotlagCfmMepIdentifier`

- `alaCfmMaCvlanListTable`
  - `alaCfmMaCvlanListIdentifier`
show ethoam domain association

Displays the information of a specific MA in a Management Domain configured on the bridge.

**show ethoam domain** *md_name* **association** *ma_name*

---

**Syntax Definitions**

- *md_name* Specifies the management domain name.
- *ma_name* Specifies the name of the Ethernet OAM Association.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ethoam domain MD association MA
Total number of MEPs configured in this MA = 1
MA-Format : string,
Primary Vlan : 100,
Associated Vlan-list : none,
Total Number of Vlans : 1,
MA-MHFstatus : mhfDefer,
MA-IdPermission : sendIdDefer,
CCM-interval : interval10s,
MEP-List(MEP-Id) : 1-5,
CVLAN-List(CVLAN-Id) : 20-30

Legend: MEP-Id: * = Inactive Endpoint
```

<table>
<thead>
<tr>
<th>MEP-ID</th>
<th>Admin State</th>
<th>Direction</th>
<th>Mac-Address</th>
<th>Port</th>
<th>Primary Vlan</th>
<th>Cvlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>enable</td>
<td>up</td>
<td>E8:E7:32:72:01:A4</td>
<td>1/1</td>
<td>200</td>
<td>30</td>
</tr>
<tr>
<td>12</td>
<td>enable</td>
<td>up</td>
<td>E8:E7:32:72:01:A4</td>
<td>1/2</td>
<td>200</td>
<td>20</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Vlan</td>
<td>The VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 will be displayed.</td>
</tr>
<tr>
<td>MA-MHFstatus</td>
<td>Indicates whether the maintenance entity can create MHFs for this MA. Options include none, explicit, or default.</td>
</tr>
<tr>
<td>CCM-interval</td>
<td>The interval between the CCM transmissions.</td>
</tr>
<tr>
<td>MEP-ID</td>
<td>Indicates the Maintenance End Point.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Indicates the administrative state (up or down) of the MEP.</td>
</tr>
<tr>
<td>Direction</td>
<td>The direction of the MEP.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the MEP.</td>
</tr>
<tr>
<td>Port</td>
<td>The slot/port number of the Bridge port to which the MEP is attached.</td>
</tr>
<tr>
<td>CVLAN-List (CVLAN-Id)</td>
<td>The CVLAN configured for the MEPs in a MA.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.
Release 8.8R1; CVLAN-List (CVLAN-Id) and Cvlan fields added in the output.

Related Commands

- **ethoam association**: Creates an Ethernet OAM Maintenance Association in the specified domain.
- **ethoam endpoint**: Creates a Maintenance End Point (MEP) and a virtual MEP.
- **ethoam association allowed-cvlan-list**: Allows to add or delete the allowed CVLANs on the Ethernet OAM Maintenance Association.

MIB Objects

- Dot1agCfmMa
  - dot1agCfmMaVid
  - dot1agCfmMaMhfCreation
  - dot1agCfmMaCcmInterval
- alaCfmMaCvlanListTable
  - alaCfmMaCvlanListIdentifier
- Dot1agCfmMep
  - dot1agCfmMepIdentifier
  - dot1agCfmMepActive
  - dot1agCfmMepDirection
  - dot1agCfmMepIfIndex
  - dot1agCfmMepMacAddress
**show ethoam domain association end-point**

Displays the information of a specific MEP in a Management Domain configured on the bridge.

```
show ethoam domain md_name association ma_name end-point mep_id
```

**Syntax Definitions**

- `md_name`: Specifies the management domain name.
- `ma_name`: Specifies the name of the Ethernet OAM Association.
- `mep_id`: Specifies the MEP of a specific MA. The valid range is 1–8191.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ethoam domain MD association MA endpoint 10
Admin State : disable,
Direction : up,
Slot/Port: virtual,
Primary VLAN : 200,
C-Vlan: 20,
MacAddress: 00:E0:B1:A0:78:A3,
Fault Notification : FNG_RESET,
CCM Enabled : disabled,
RFP Status : enabled,
CCM Linktrace Priority : 7,
CCM Not Received : false,
CCM Error defect : false,
CCM Xcon defect : false,
MEP RDI defect : false,
MEP Last CCM Fault : not specified,
MEP Xcon Last CCM Fault : not specified,
MEP Error Mac Status : false,
MEP Lbm NextSeqNumber : 0,
MEP Ltm NextSeqNumber : 32157,
```
Fault Alarm Time : 250,
Fault Reset Time : 1000,
Lowest PrDefect Allowed : DEF_MAC_REM_ERR_XCON,
Highest PrDefect Present : DEF_NONE
<table>
<thead>
<tr>
<th><strong>output definitions</strong></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin State</strong></td>
<td>Indicates the administrative state <em>(up or down)</em> of the MEP.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td>The direction of the MEP.</td>
</tr>
<tr>
<td><strong>Slot/Port</strong></td>
<td>The slot/port number of the Bridge port to which the MEP is attached. If the value is virtual, it indicates a virtual port.</td>
</tr>
<tr>
<td><strong>Primary Vlan</strong></td>
<td>The Primary VLAN ID monitored by this MA. If the MA is not attached to any VLAN, 0 is displayed.</td>
</tr>
<tr>
<td><strong>C-Vlan</strong></td>
<td>The CVLAN configured for a MEP if it's a CVLAN MEP. If the MEP is SVLAN then this field will be displayed as `-`.</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>The MAC address of the MEP.</td>
</tr>
<tr>
<td><strong>Fault Notification</strong></td>
<td>Indicates the current state of the MEP Fault Notification Generator State Machine, which can be FNG_RESET, FNG_DEFECT, FNG_REPORT_DEFECT, FNG_DEFECT_REPORTED, or FNG_DEFECT_CLEARING.</td>
</tr>
<tr>
<td><strong>RFP Status</strong></td>
<td>Indicates the status of the RFP.</td>
</tr>
<tr>
<td><strong>CCM Enabled</strong></td>
<td>Indicates whether the MEP generates CCMs <em>(enabled)</em> or not <em>(disabled)</em>.</td>
</tr>
<tr>
<td><strong>CCM Linktrace Priority</strong></td>
<td>Indicates the priority value for CCMs and LTMs transmitted by the MEP.</td>
</tr>
<tr>
<td><strong>CCM Not Received</strong></td>
<td>Indicates if CCMs are not being received <em>(true)</em> or received <em>(false)</em> from at least one of the configured remote MEPs.</td>
</tr>
<tr>
<td><strong>CCM Error defect</strong></td>
<td>Indicates if a stream of erroneous CCMs is being received <em>(true)</em> or not <em>(false)</em> from a MEP in this MA.</td>
</tr>
<tr>
<td><strong>CCM Xcon defect</strong></td>
<td>Indicates if a stream of CCMs is being received <em>(true)</em> or not <em>(false)</em> from a MEP that belongs to another MA.</td>
</tr>
<tr>
<td><strong>MEP RDI Received</strong></td>
<td>Indicates that any other MEP in this MA is transmitting the RDI bit. Options include true or false.</td>
</tr>
<tr>
<td><strong>MEP Last CCM Fault</strong></td>
<td>The last-received CCM that triggered a MA fault.</td>
</tr>
<tr>
<td><strong>MEP Xcon Last CCM Fault</strong></td>
<td>The last-received CCM that triggered a cross-connect fault.</td>
</tr>
<tr>
<td><strong>MEP Error Mac Status</strong></td>
<td>Indicates a port status TLV. Options include true or false.</td>
</tr>
<tr>
<td><strong>MEP Lbm NextSeqNumber</strong></td>
<td>The next Transaction Identifier or Sequence Number to be sent in an LBM.</td>
</tr>
<tr>
<td><strong>MEP Ltm NextSeqNumber</strong></td>
<td>The next Transaction Identifier or Sequence Number to be sent in an LTM.</td>
</tr>
<tr>
<td><strong>Fault Alarm Time</strong></td>
<td>The time interval during which one or more defects should be detected before the fault alarm is issued</td>
</tr>
<tr>
<td><strong>Fault Reset Time</strong></td>
<td>The time interval during which the fault alarm is re-enabled to process faults.</td>
</tr>
<tr>
<td><strong>Lowest PrDefect Allowed</strong></td>
<td>The lowest priority defect that allowed to generate fault alarm.</td>
</tr>
<tr>
<td><strong>Highest PrDefect Present</strong></td>
<td>The highest priority defect since the MEPs Fault Notification Generator in reset state.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.3.1; command was introduced.
Release 8.8R1; C-Vlan field added in the output.

**Related Commands**

- `ethoam endpoint` Creates an Ethernet OAM Maintenance End Point in the specified MA.
- `ethoam endpoint admin-state` Configures the administrative state of MEP.

**MIB Objects**

- `Dot1agCfmMep`  
  - `dot1agCfmMepActive`
  - `dot1agCfmMepDirection`
  - `dot1agCfmMepPortNumber`
  - `dot1agCfmMepMacAddress`
  - `dot1agCfmMepFngState`
  - `dot1agCfmMepCcmEnabled`
  - `dot1agCfmMepCcmLtmiPriority`
  - `dot1agCfmMepSomeRmepCcmDefect`
  - `dot1agCfmMepErrorCcmDefect`
  - `dot1agCfmMepXconCcmDefect`
  - `dot1agCfmMepSomeRdiDefect`
  - `dot1agCfmMepErrorCcmLastFailure`
  - `dot1agCfmMepXconCcmLastFailure`
  - `dot1agCfmMepErrMacStatus`
  - `dot1agCfmMepLtmNextSeqNumber`
  - `dot1agCfmMepFngAlarmTime`
  - `dot1agCfmMepFngAlarmTime`
  - `dot1agCfmMepLowPrDef`
  - `dot1agCfmMepHighestPrDefect`

- `alaCfmMepTable`
  - `alaCfmMepCvlanId`
show ethoam default-domain configuration

Displays the level, MHF, and ID permission values for the default domain.

show ethoam default-domain configuration

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ethoam default-domain configuration
Level : 3,
MHF-Creation : mhfdefault,
ID-Permission : sendIdnone

output definitions

<table>
<thead>
<tr>
<th>Level</th>
<th>The level assigned to the default domain. Configured through the ethoam default-domain level command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MHF-creation</td>
<td>Indicates the MHF value for a VLAN that is part of the default MD Options include none, explicit, or default. Configured through the ethoam default-domain mhf command.</td>
</tr>
<tr>
<td>ID-Permission</td>
<td>The ID permission of the default domain. Configured through the ethoam default-domain id-permission command.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.
**Related Commands**

(show ethoam default-domain) Displays the primary VLAN configuration for the default domain.

**MIB Objects**

dot1agCfmMaDefaultMdDefLevel
  dot1agCfmMaDefaultMdDefMhfCreation
  dot1agCfmMaDefaultMdDefIdPermission
show ethoam default-domain

Displays all the default MD information for all the primary VLANs or for a specific primary VLAN.

show ethoam default-domain [primary-vlan vlan_id]

Syntax Definitions

vlan_id
The primary VLAN ID.

Defaults

By default, the default MD information for all primary VLANs is displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the vlan_id parameter with this command to view information about the default MD for a specific primary VLAN.

Examples

-> show ethoam default-domain

<table>
<thead>
<tr>
<th>Primary-Vlan</th>
<th>Mhf-creation</th>
<th>Level</th>
<th>Id-Permission</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>mhfDefer</td>
<td>no-level</td>
<td>sendIdDefer</td>
<td>true</td>
</tr>
<tr>
<td>10</td>
<td>mhfDefault</td>
<td>3</td>
<td>sendIdNone</td>
<td>true</td>
</tr>
</tbody>
</table>

-> show ethoam default-domain primary-vlan 10

<table>
<thead>
<tr>
<th>Primary-Vlan</th>
<th>Mhf-creation</th>
<th>Level</th>
<th>Id-Permission</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>mhfDefault</td>
<td>3</td>
<td>sendIdNone</td>
<td>true</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Primary Vlan</th>
<th>The primary VLAN ID of the default MD.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mhf-creation</td>
<td>The primary VLAN ID MHF value (none, explicit, or default).</td>
</tr>
<tr>
<td>Level</td>
<td>The primary VLAN level (no-level, 0–7).</td>
</tr>
<tr>
<td>Id-Permission</td>
<td>The primary VLAN ID permission (none, chassid, or defer).</td>
</tr>
</tbody>
</table>
Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam default-domain

Modifies the default domain for the specified primary VLAN.

primary-vlan

MIB Objects

DotlagCfmDefaultMdLevel
  dotlagCfmDefaultMdLevelVid
  dotlagCfmDefaultMdLevelMhfCreation
  dotlagCfmDefaultMdLevelLevel
**show ethoam remote-endpoint domain**

Displays the information of all remote MEPs learned as a part of the CCM message exchange.

**show ethoam remote-endpoint domain** *md_name association ma_name end-point s_mepid [remote-mep r_mepid]*

---

**Syntax Definitions**

- **md_name**: Specifies the domain name.
- **ma_name**: Specifies the name of the Ethernet OAM Association.
- **s_mepid**: Specifies the MEP of a specific MA. The valid range is 1–8191.
- **r_mepid**: The remote MEP. The valid range is 1–8191.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> show ethoam remote-endpoint domain MD association MA end-point 10

Legends: PortStatusTlv: 1 = psBlocked, 2 = psUp, 0 = psNoTlv
InterfaceStatusTlv: 1 = ifUp, 2 = ifDown, 4 = ifUnknown, 0=ifNoTlv

<table>
<thead>
<tr>
<th>RMEP-ID</th>
<th>RMEP Status</th>
<th>OkFailed</th>
<th>Mac Address</th>
<th>port I/f</th>
<th>RDI</th>
<th>Ch-id</th>
<th>Ch-id Tlv</th>
<th>Tlv</th>
<th>value</th>
<th>Subtype</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>RMEP_OK</td>
<td></td>
<td>00:E0:B1:6E:41:65</td>
<td>2</td>
<td>1</td>
<td>false</td>
<td>LCL-ASND DUT-1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>RMEP_OK</td>
<td></td>
<td>00:E0:B1:6E:41:64</td>
<td>2</td>
<td>1</td>
<td>false</td>
<td>LCL-ASND DUT-2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**output definitions**

- **MEP-ID**: Indicates the Maintenance End Point.
- **RMEP Status**: The operational state of the remote MEP Remote State machines for this MEP, which can be **RMEP_IDLE**, **RMEP_START**, **RMEP_FAILED**, or **RMEP_OK**.
**output definitions (continued)**

| **OkFailed Time** | The time (SysUpTime) when the Remote MEP state machine last entered either the RMEP_FAILED or RMEP_OK. |
| **MacAddress** | The MAC address of the remote MEP. |
| **Port Status Tlv** | The MAC status TLV last received. |
| **I/f Status Tlv** | The interface status TLV last received. |

**Note:** Output shown above is not accurate as it is adjusted to display it in the single row. Following are modified:
- P/S Tlv - Port Status Tlv
- I/F Tlv - I/F Status Tlv
- Ch-id Subtype - Chassis ID Subtype
- Ch-id - Chassis ID
- LCL-ASND - LOCALLY_ASSIGNED

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show ethoam domain association end-point` Displays the information of a specific MEP in a Management Domain configured on the bridge.

**MIB Objects**

- `dotlagCfmMepDbTable`
  - `dotlagCfmMepDbRmepIdentifier`
  - `dotlagCfmMepDbRmepState`
  - `dotlagCfmMepDbRmepFailedOkTime`
  - `dotlagCfmMepDbRdi`
  - `dotlagCfmMepDbPortStatusTlv`
  - `dotlagCfmMepDbInterfaceStatusTlv`
  - `dotlagCfmMepDbChassisIdSubtype`
  - `dotlagCfmMepDbChassisId`
**show ethoam cfmstack**

Displays the contents of CFM Stack Managed Object, which determines the relationships among MEPs and MIPs on a specific bridge port.

```
show ethoam cfmstack {port chassis/slot/port | virtual | linkagg agg_id}
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port**: Slot and port number for which the contents of the configured MEP or MIP will be displayed.
- **virtual**: Virtual port.
- **agg_id**: The aggregate ID for which the contents of the configured MEP or MIP will be displayed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `-> show ethoam cfmstack port 1/1/2`
  MEP-Id 1 - Vlan 100:
  - Direction: up,
  - MAC-Address: 00:D0:95:01:2C:EB,
  - Maintenance Association: ma,
  - Maintenance Domain: md,
  - MD-level: 7
  - Cvlan : 200

- `-> show ethoam cfmstack port virtual`
  MEP-Id 32 - Vlan 30:
  - Direction: up,
  - MAC-Address: 00:E0:B1:A5:F2:34,
  - Maintenance Association: MA4,
  - Maintenance Domain: MD4,
MD-level: 4

### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vlan-id</strong></td>
<td>The VLAN ID to which the MEP is attached.</td>
</tr>
<tr>
<td><strong>Direction</strong></td>
<td>Indicates the direction (Inward or Outward) of the Maintenance Point (MP) on the Bridge port.</td>
</tr>
<tr>
<td><strong>MAC-Address</strong></td>
<td>The MEP ID configured on this port.</td>
</tr>
<tr>
<td><strong>Maintenance Domain</strong></td>
<td>The name of the maintenance domain.</td>
</tr>
<tr>
<td><strong>Maintenance Association</strong></td>
<td>The name of the maintenance association.</td>
</tr>
<tr>
<td><strong>MD-level</strong></td>
<td>The MD level at which the MD was created.</td>
</tr>
<tr>
<td><strong>Cvlan</strong></td>
<td>The CVLAN configured for the MEPs in a MA.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.3.1; command was introduced.
Release 8.8R1; CVLAN field added in the output.

### Related Commands

**ethoam endpoint admin-state**

Creates an Ethernet OAM Maintenance End Point in the specified MA.

### MIB Objects

- **DotlagCfmMd**
  - dotlagCfmMdName
- **DotlagCfmMa**
  - dotlagCfmMaName
- **DotlagCfmStack**
  - dotlagCfmStackVlanIdOrNone
  - dotlagCfmStackDirection
  - dotlagCfmStackMacAddress
  - dotlagCfmStackMdLevel
show ethoam linktrace-reply

Displays the content of the Linktrace reply (LTR) returned by a previously transmitted LTM. This command displays the LTR based on the transaction identifier or sequence number of the LTM for which the LTR is to be displayed.

show ethoam linktrace-reply domain md_name association ma_name endpoint s_mepid tran-id num

Syntax Definitions

- **md_name**: Specifies the domain name.
- **ma_name**: Name of the Ethernet OAM Association.
- **s_mepid**: Specifies the MEP for which the LTR is to be displayed. The valid range is 1-8191.
- **num**: Specifies the Transaction ID or sequence number returned from a previously transmitted LTM.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- “LTM operation successful. Target is reachable.” – This message suggests that LTM has reached the target and all the expected LTRs have been received.
- “LTM operation unsuccessful. Target not reachable.” – This message suggests that LTM is successfully initiated but the target is not reachable.
- “LTM operation unsuccessful. Target is reachable.” – This message suggest that Target is reachable but at least one of the LTR from intermediate hop is not received.
- “LTM operation in progress.” – This message suggests that LTM operation is in progress. This message will appear if show CLI is fired before LTM Time-out time.
- “LTM Timed out.”- This message suggests that either LTM is not initiated properly or when none of the expected LTRs is received in LTM Time-out duration which is 5 seconds.
Examples

-> show ethoam linktrace-reply domain MD association MA endpoint 10 tran-id 1256
LTM operation successful. Target is reachable.
Ttl : 63,
   LTM Forwarded : yes,
   Terminal MEP : no,
   Last Egress Identifier : 00-00:00:D0:95:EA:79:62,
   Next Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
   Relay Action : RLY_FDB,
   Chassis ID Subtype : LOCALLY_ASSIGNED,
   Chassis ID : DUT-2,
   Ingress Action : ING_OK,
   Ingress Mac : 00:D0:95:EA:9E:D4,
   Ingress Port ID Subtype : LOCALLY_ASSIGNED,
   Ingress Port ID : 1/1,
   Egress Action : EGR_OK,
   Egress Mac : 00:D0:95:EA:9E:D5,
   Egress Port ID Subtype : LOCALLY_ASSIGNED,
   Egress Port ID : 1/2

Ttl : 62,
   LTM Forwarded : no,
   Terminal MEP : yes,
   Last Egress Identifier : 00-00:00:D0:95:EA:9E:BA,
   Next Egress Identifier : 00-00:00:00:00:00:00:00,
   Relay Action : RLY_HIT,
   Chassis ID Subtype : LOCALLY_ASSIGNED,
   Chassis ID : DUT-3,
   Ingress Action : ING_OK,
   Ingress Mac : 00:D0:95:EA:AB:D2,
   Ingress Port ID Subtype : LOCALLY_ASSIGNED,
   Ingress Port ID : 1/1,
   Egress Action : EGR_NONE,
   Egress Mac : 00:00:00:00:00:00:00,
   Egress Port ID Subtype : NONE,
   Egress Port ID : none

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ttl</td>
<td>Time to live field for the returned LTR.</td>
</tr>
<tr>
<td>LTM Forwarded</td>
<td>Indicates whether the LTM was forwarded or not.</td>
</tr>
<tr>
<td>Terminal MEP</td>
<td>Indicates whether the MP reported in the reply Ingress/Egress TLV is a MEP.</td>
</tr>
<tr>
<td>Last Egress Identifier</td>
<td>Identifies the MEP linktrace initiator that originated, or the responder that forwarded, the LTM to which this LTR is the response.</td>
</tr>
<tr>
<td>Next Egress Identifier</td>
<td>Identifies the linktrace responder that transmitted this LTR, and can forward the LTM to the next hop.</td>
</tr>
<tr>
<td>Relay Action</td>
<td>Indicates how the dataframe targeted by the LTM would be passed to Egress bridge port. Options include RLY_HIT, RLY_FDB, or RLY_MPDB.</td>
</tr>
<tr>
<td>Ingress Action</td>
<td>Indicates how the dataframe targeted by the LTM would be received on the receiving MP. Options include ING_NONE, ING_OK, ING_DOWN, ING_BLOCKED, or ING_VID.</td>
</tr>
<tr>
<td>Ingress Mac</td>
<td>The MAC address returned in the ingress MAC address field.</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Egress Action</th>
<th>Indicates how the dataframe targeted by the LTM would be passed through Egress bridge port. Options include ING_NONE, ING_OK, ING_DOWN, ING_BLOCKED, or ING_VID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress Mac</td>
<td>The MAC address returned in the egress MAC address field.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam linktrace Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

MIB Objects

DotlagCfmLtr
  dotlagCfmLtrTtl
  dotlagCfmLtrForwarded
  dotlagCfmLtrTerminalMep
  dotlagCfmLtrLastEgressIdentifier
  dotlagCfmLtrNextEgressIdentifier
  dotlagCfmLtrRelay
  dotlagCfmLtrIngress
  dotlagCfmLtrIngressMac
  dotlagCfmLtrEgress
  dotlagCfmLtrEgressMac
show ethoam linktrace-tran-id

Displays the transaction identifiers returned by previously generated LTM from a specified MEP.

show ethoam linktrace-tran-id domain {md_name | mac_address} association ma_name endpoint mep_id

Syntax Definitions

- **md_name**: Specifies the domain name.
- **mac_address**: Specifies the CFM system MAC address.
- **ma_name**: Name of the Ethernet OAM Association.
- **mep_id**: Specifies the MEP for which the LTR is to be displayed. The valid range is 1-8191.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ethoam linktrace-tran-id domain esd.ale.com association ale-sales endpoint 3

S.No | Transaction Id
-----|------------------
 1    | 13357,           
 2    | 13358,           
 3    | 13359,           

**output definitions**

- **S.No**: Indicates the sequence number.
- **Transaction Id**: Indicates the Transaction Identifier returned from a previously transmitted LTM.
**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **ethoam linktrace**

  Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

**MIB Objects**

- **DotlagCfmLtr**
  - **dotlagCfmLtrSeqNumber**

show ethoam vlan

Displays the Ethernet OAM statistics of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

show ethoam vlan vlan_id

Syntax Definitions

vlan_id

VLAN ID, primary or non-primary VID (e.g. ‘10’).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ethoam vlan 10
Primary Vlan : 10,
Associated Vlan-list : 15-20 25 50-80

-> show ethoam vlan 15
Primary Vlan : 10,
Associated Vlan-list : 15-20 25 50-80

Release History

Release 7.3.1; command was introduced.
Related Commands

**ethoam endpoint**  
Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

- `dot1agCfmMaVlanTable`
- `dot1agCfmVlanVid`
- `dot1agCfmVlanPrimaryVid`
**show ethoam statistics**

Displays the Ethernet OAM of all the Management Domains configured on the bridge. Also, displays the statistics of all the MAs and matching MEPs for all the MDs.

```
show ethoam statistics domain {md_name | mac_address} [association ma_name] [end-point mep_id]
```

**Syntax Definitions**

- **md_name**: Specifies the domain name.
- **mac_address**: Specifies the CFM system MAC address.
- **ma_name**: Specifies the name of Ethernet OAM Association.
- **mep_id**: Specifies a MEP for a specific MA.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show ethoam statistics domain MD
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected   MA
Out    Error    In   of order  Out     MSDU    LTR In
-----------------------------------------------
3    105       0      0        0      0        0          0  MA

-> show ethoam statistics domain MD association MA
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected
Out    Error    In   of order  Out     MSDU    LTR In
-----------------------------------------------
3    105       0      0        0      0        0          0

-> show ethoam statistics domain MD association MA endpoint 3
MEP-ID  CCM   CCM Seq   LBR   LBR Out  LBR   LBR Bad  Unexpected
Out    Error    In   of order  Out     MSDU    LTR In
-----------------------------------------------
3    105       0      0        0      0        0          0
```
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEP-Id</td>
<td>The MEP ID configured in the specified MA.</td>
</tr>
<tr>
<td>CCM Out</td>
<td>The total number of CCMs transmitted.</td>
</tr>
<tr>
<td>CCM Seq Error</td>
<td>The total number of out-of-sequence CCMs received from all remote MEps.</td>
</tr>
<tr>
<td>LBR In</td>
<td>The total number of valid, in-order LBRs received.</td>
</tr>
<tr>
<td>LBR Out of order</td>
<td>The total number of valid, out-of-order LBRs received.</td>
</tr>
<tr>
<td>LBR Out</td>
<td>The total number of LBRs transmitted.</td>
</tr>
<tr>
<td>LBR Bad MSDU</td>
<td>The total number of LBRs received whose mac_service_data_unit did not match.</td>
</tr>
<tr>
<td>Unexpected LTR In</td>
<td>The total number of unexpected LTRs received.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

ethoam endpoint

Enables the maintenance entity to initiate transmitting loopback messages (LBMs) and obtaining loopback replies.

MIB Objects

DotlagCfmMep

<table>
<thead>
<tr>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>dotlagCfmMepIdentifier</td>
</tr>
<tr>
<td>dotlagCfmMepCcmOut</td>
</tr>
<tr>
<td>dotlagCfmMepRccmSequenceErrors</td>
</tr>
<tr>
<td>dotlagCfmMepLbrIn</td>
</tr>
<tr>
<td>dotlagCfmMepLbrInOutOfOrder</td>
</tr>
<tr>
<td>dotlagCfmMepLbrOut</td>
</tr>
<tr>
<td>dotlagCfmMepLbrBadMsdu</td>
</tr>
<tr>
<td>dotlagCfmMepUnexpLtrIn</td>
</tr>
</tbody>
</table>
show ethoam config-error

Displays the configuration error for a specified VLAN and port or linkagg.

show ethoam config-error [vlan vlan_id] [port chassis/slot/port | linkagg agg_id]

Syntax Definitions

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_id</td>
<td>VLAN Identifier.</td>
</tr>
<tr>
<td>chassis</td>
<td>The chassis identifier.</td>
</tr>
<tr>
<td>slot/port</td>
<td>Physical slot and port number.</td>
</tr>
<tr>
<td>agg_id</td>
<td>Logical link aggregate ID number.</td>
</tr>
</tbody>
</table>

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ethoam config-error
Vlan Port Error-type
--------------
10 1/2 CFMleak
10 1/10 CFMleak
30 1/2 CFMleak

-> show ethoam config-error vlan 10
vlan port error-type
--------------
10 1/2 CFMleak
10 1/10 CFMleak

-> show ethoam config-error port 1/2
vlan port error-type
--------------
10 1/2 CFMleak
30 1/2 CFMleak
-> show ethoam config-error vlan 10 port 1/2

<table>
<thead>
<tr>
<th>vlan</th>
<th>port</th>
<th>error-type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>1/2</td>
<td>CFMleak</td>
</tr>
</tbody>
</table>

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>VLAN identifier number.</td>
</tr>
<tr>
<td>port</td>
<td>Physical slot and port number.</td>
</tr>
<tr>
<td>error-type</td>
<td>Type of an error.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- **ethoam linktrace** Enables the maintenance entity to initiate transmitting of Link Trace Messages (LTM).

**MIB Objects**

- dotlagCfmConfigErrorListTable
- dotlagCfmConfigErrorListVid
- dotlagCfmConfigErrorListIfIndex
- dotlagCfmConfigErrorListErrorType
show ethoam one-way-delay

Displays the one-way ETH-DM delay (latency) and jitter parameters either for all entries or for a specified MAC address for a particular source MEP-ID.

show ethoam one-way-delay domain \textit{md\_name} association \textit{ma\_name} endpoint \textit{s\_mepid} [mac-address \textit{mac\_address}]

**Syntax Definitions**

- \textit{md\_name} Specifies the domain name. For more information on the different formats of the domain name, refer to \texttt{ethoam domain}.
- \textit{ma\_name} Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.
- \textit{s\_mepid} Source MEP ID. The valid range is 1–8191.
- \textit{mac\_address} MAC Address of the remote MEP.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Dash (‘-’) in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown. This will happen only when 1DM is received for the first time.
- Maximum entries that Delay Result table can store are 1024. After that, the oldest entry is deleted from the table whenever a new entry is required.

**Examples**

\texttt{-}\texttt{> show ethoam one-way-delay domain MD association MA endpoint 10}

Legend: Jitter: - = undefined value

<table>
<thead>
<tr>
<th>Remote Mac address</th>
<th>Delay (us)</th>
<th>Jitter (us)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:d0:95:ef:44:44</td>
<td>2369</td>
<td>1258</td>
</tr>
<tr>
<td>00:d0:95:ef:66:88</td>
<td>5896</td>
<td>282</td>
</tr>
<tr>
<td>00:d0:95:ef:88:88</td>
<td>2584</td>
<td>-</td>
</tr>
<tr>
<td>00:d0:95:ef:66:55</td>
<td>2698</td>
<td>4782</td>
</tr>
</tbody>
</table>
-> show ethoam one-way-delay domain MD association MA endpoint 10 mac-address 00:d0:95:ef:44:44

Legend: Jitter: - = undefined value

Remote Mac address       Delay (us)   Jitter (us)
--------------------+-------------+-------------------
00:d0:95:ef:44:44        2369           1258

output definitions

<table>
<thead>
<tr>
<th>Remote Mac address</th>
<th>Delay</th>
<th>Jitter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote MAC address</td>
<td>Physical slot and port number.</td>
<td>Type of an error.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.

Related Commands

**ethoam one-way-delay** Initiates one-way-delay messages from a particular MEP to an RMEP.

MIB Objects

- dotlagCfmMdTable
  - dotlagCfmMdName
- dotlagCfmMaNetTable
  - dotlagCfmMaNetName
- dotlagCfmMepTable
  - dotlagCfmMepIdentifier
- alaDotlagCfmMepDelayRsltTable
  - alaDotlagCfmMepDelayRMepMacAddress
  - alaCfmMepDelayTestType
  - alaCfmMepDelayTestDelay
  - alaCfmMepDelayVariation
show ethoam two-way-delay

Displays the two-way ETH-DM delay and jitter parameters for a specific remote MAC-Address or for all the MAC-Addresses for which two-way-delay was initiated for a particular source MEP-ID.

show ethoam two-way-delay domain md_name association ma_name endpoint s_mepid [mac-address mac_address]

Syntax Definitions

**md_name**
Specifies the domain name. For more information on the different formats of the domain name, refer to `ethoam domain`.

**ma_name**
Name of the Ethernet OAM Association. Up to 48 (minus the domain name length) characters may be used.

**s_mepid**
Source MEP ID. The valid range is 1–8191.

**mac_address**
MAC Address of the remote MEP.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If ‘0’ appears in the output in RMEP-ID column signifies that the DMM was initiated with target-macaddress. As multiple RMEPs can have same mac-address.

- If a dash (‘-‘) appears in the output in Jitter column signifies that the value can not be calculated as the previous delay value is unknown, i.e. if only one reply for DMM (DMR) is received and this was the first time DMM was initiated from the MEP, then jitter will not be calculated.

- Maximum entries that Delay Result table can store are 1024. After that, the DMM request shall be rejected if a new entry needs to be created for the MEP. If entry for the MEP already exists in the table, that entry shall be updated with the new one.
Examples

-> show ethoam two-way-delay domain MD association MA endpoint 10 mac-address 00:d0:95:ef:44:44
Legend: Jitter: - = undefined value
: RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
-------------------+--------+--------------+------------
00:d0:95:ef:44:44  12       2369         1258

-> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 0
Legend: Jitter: - = undefined value
: RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
-------------------+--------+--------------+------------
00:d0:95:ef:66:88   0       5896         282
00:d0:95:ef:88:88   0       2584        1856

-> show ethoam two-way-delay domain MD association MA endpoint 10 remote-mep 15
Legend: Jitter: - = undefined value
: RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
-------------------+--------+--------------+------------
00:d0:95:ef:66:55   15       2736         -

-> show ethoam two-way-delay domain MD association MA endpoint 10
Legend: Jitter: - = undefined value
: RMEP-ID: 0 = two-way-delay was initiated with target mac-address

Remote Mac address  RMEP-ID  Delay (us)  Jitter (us)
-------------------+--------+--------------+------------
00:d0:95:ef:44:44  12       2369        1258
00:d0:95:ef:66:88   0       5896         282
00:d0:95:ef:88:88   0       2584        1856
00:d0:95:ef:66:55   15       2736         -

output definitions

Remote Mac address  Remote MAC address.
RMEP-ID            Value of RMEP-ID
Delay              Physical slot and port number.
Jitter             Type of an error.

Release History

Release 7.3.1; command was introduced.
**Related Commands**

**ethoam two-way-delay**

Initiate two-way-delay messages from a particular MEP to an RMEP using target-endpoint or target-MAC address.

**MIB Objects**

dot1agCfmMdTable
dot1agCfmMdName
dot1agCfmMaNetTable
dot1agCfmMaNetName
dot1agCfmMepTable
dot1agCfmMepIdentifier
alaDot1agCfmMepDelayRsltTable
alaCfmMepDelayRMepMacAddress
alaCfmMepDelayTestType
alaCfmMepDelayTestDelay
alaDot1agCfmMepDelayVariation
54 LINK OAM Commands

Ethernet in the First Mile (EFM), also known as LINK OAM, is a collection of protocols specified in IEEE 802.3ah, defining Ethernet in the access networks that connects subscribers to their immediate service provider. EFM, EFM-OAM and LINKOAM refers to IEEE 802.3ah standard.

LINK OAM (operation, administration, and maintenance) is a tool which monitors Layer-2 link status on the network by sending OAM protocol data units (OAMPDU$s) between the network devices. OAMPDU$s contain control and status information used to monitor, test and troubleshoot OAM-enabled links. By enabling LINK OAM on switch ports, network administrators can monitor the link-related issues on the first mile. LINK OAM provides network administrators the ability to monitor link performance, remote fault detection and remote loopback control.

**Note.** EFM (LINK OAM) does not include functions such as station management, bandwidth allocation or provisioning functions.

MIB information for the EFM (LINK OAM) commands is as follows:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>alcatel-ind1-dot3-oam-mib.mib</td>
<td>ALCATEL-IND1-DOT3-OAM-MIB</td>
</tr>
<tr>
<td>dot3-oam-mib.mib</td>
<td>DOT3-OAM-MIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>Global Configuration Commands</th>
<th>efm-oam admin-state</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>efm-oam multiple-pdu-count</td>
</tr>
<tr>
<td></td>
<td>efm-oam errored-frame-seCONDS-summary</td>
</tr>
<tr>
<td></td>
<td>efm-oam errored-frame-period</td>
</tr>
<tr>
<td></td>
<td>efm-oam errored-frame</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Status Commands</th>
<th>efm-oam port admin-state</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>efm-oam port mode</td>
</tr>
<tr>
<td></td>
<td>efm-oam port propagate-events</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Event Notification Commands</th>
<th>efm-oam errored-frame</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>efm-oam errored-frame-period</td>
</tr>
<tr>
<td></td>
<td>efm-oam errored-frame-seCONDS-summary</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Timer Interval Commands</th>
<th>efm-oam port keepalive-interval</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>efm-oam port hello-interval</td>
</tr>
</tbody>
</table>
### Remote Loopback Commands
- `efm-oam port remote-loopback`
- `efm-oam port remote-loopback start`
- `efm-oam port l1-ping`

### Show Commands
- `show efm-oam port`
- `show efm-oam port detail`
- `show efm-oam port remote detail`
- `show efm-oam port history`
- `show efm-oam port l1-ping detail`
- `show efm-oam port statistics`
- `show efm-oam configuration`

### Clear Commands
- `clear efm-oam statistics`
- `clear efm-oam log-history`
**efm-oam admin-state**

Enables or disables the LINK OAM protocol on the switch.

`efm-oam admin-state {enable | disable}`

---

**Syntax Definitions**

- **enable**
  - Enables the LINK OAM protocol.
- **disable**
  - Disables the LINK OAM protocol.

**Defaults**

By default, the LINK OAM protocol is disabled for the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- LINK OAM must be enabled globally for the OAM to be functional on all the ports.
- When LINK OAM is disabled globally, all dynamically learned information on the port, including peer information, is deleted. However, the LINK OAM configuration for the port is retained.

**Examples**

- `-> efm-oam admin-state enable`
- `-> efm-oam admin-state disable`

**Release History**

Release 8.5R4; command was introduced.
**Related Commands**

- **efm-oam port admin-state** Enables or disables LINK OAM protocol on the specified port or on a range of ports.
- **efm-oam port mode** Configures the LINK OAM mode on the port or on the range of ports to active or passive.
- **show efm-oam configuration** Displays the global LINK OAM configuration.

**MIB Objects**

- **alaDot3OamStatus**
**efm-oam port admin-state**

Enables or disables LINK OAM protocol on the specified port or on a range of ports.

```plaintext
efm-oam port chassis/slot/port[-port2] admin-state {enable | disable}
```

### Syntax Definitions
- **chassis**: The chassis identifier.
- **slot/port**: The slot number of the module and the physical port number on that module.
- **-port2**: Specifies the last port in the range of ports.
- **enable**: Enables LINK OAM protocol on the specified port.
- **disable**: Disables LINK OAM protocol on the specified port.

### Defaults
By default, the LINK OAM protocol is disabled on all ports for the switch.

### Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines
- LINK OAM must be enabled globally for the OAM to be functional on all the ports.
- If LINK OAM is disabled for the port or globally disabled for the switch, any OAMPDUs received are discarded.
- When LINK OAM is disabled for the port, all dynamically learned information on the port, including peer information, is deleted. However, the LINK OAM configuration for the port is retained.
- LINK OAM is not supported on the mirroring ports.
- In link aggregates, LINK OAM is supported on an individual aggregable port only.

### Examples
- `-> efm-oam port 1/1/1 admin-state enable`
- `-> efm-oam port 1/1/1 admin-state disable`
- `-> efm-oam port 2/1/1-10 admin-state enable`
- `-> efm-oam port 2/1/1-4 admin-state disable`
**Release History**
Release 8.5R4; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>efm-oam port mode</td>
<td>Configure a LINK OAM mode on the port or on the range of ports to active or passive.</td>
</tr>
<tr>
<td>show efm-oam configuration</td>
<td>Displays the global LINK OAM configuration.</td>
</tr>
<tr>
<td>show efm-oam port</td>
<td>Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.</td>
</tr>
<tr>
<td>show efm-oam port detail</td>
<td>Displays the configuration and other related parameters for a port.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- dot3OamTable
  - dot3OamAdminState
**efm-oam port mode**

Configures the LINK OAM mode on the port or on the range of ports to active or passive.

`efm-oam port chassis/slot/port[-port2] mode {active | passive}`

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port`: The slot number for the module and the physical port number on that module.
- `-port2`: Specifies the last port in the range of ports.
- `active`: Configures the LINK OAM mode to active.
- `passive`: Configures the LINK OAM mode to passive.

**Defaults**

By default, LINK OAM mode is set to active on all ports.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- LINK OAM discovery process is never initiated from a port when it is in passive mode. At least one of the two peer ports should be in active mode.
- An active port will respond to Loopback-control OAMPDUs only if the peer EFM-OAM client is also in active mode.

**Examples**

- `-> efm-oam port 1/1/1 mode active`
- `-> efm-oam port 1/1/1 mode passive`
- `-> efm-oam port 2/1/1-10 mode active`
- `-> efm-oam port 2/1/1-4 mode passive`

**Release History**

Release 8.5R4; command was introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>efm-oam port admin-state</code></td>
<td>Enables or disables LINK OAM protocol on the specified port or on a range of ports.</td>
</tr>
<tr>
<td><code>show efm-oam port</code></td>
<td>Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.</td>
</tr>
<tr>
<td><code>show efm-oam configuration</code></td>
<td>Displays the global LINK OAM configuration.</td>
</tr>
</tbody>
</table>

### MIB Objects

- `dot3OamTable
  - dot3OamMode`
**efm-oam port keepalive-interval**

Configures the timeout interval for the dynamically learned neighboring devices on a port or on a range of ports. Keepalive-interval is the maximum time period for which a LINK OAM port shall wait for a hello message from its peer before resetting a discovery session.

**efm-oam port chassis/slot/port[-port2] keepalive-interval seconds**

### Syntax Definitions

- `chassis` The chassis identifier.
- `slot/port` The slot number for the module and the physical port number on that module.
- `-port2` Specifies the last port in the range of ports.
- `seconds` Specifies the keep-alive interval value in seconds. The range for this interval is 5 to 120 seconds.

### Defaults

By default, the keep-alive interval value is 5 seconds.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>9900</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Even if unsupported OAMPDU is received on the port, keep-alive timer is reset on the port.
- To set the timer to its default value, set 5 seconds as the keepalive-interval.

### Examples

- `efm-oam port 1/1/1 keepalive-interval 10`
- `efm-oam port 2/1/1-10 keepalive-interval 10`

### Release History

Release 8.5R4; command was introduced.
**Related Commands**

- `efm-oam port hello-interval`  
  Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of a LINK OAM enabled port.

- `show efm-oam port detail`  
  Displays the configuration and other related parameters for a port.

**MIB Objects**

- `alaDot3OamTable`  
  - `alaDot3OamKeepAliveInterval`
efm-oam port hello-interval

Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of an LINK OAM enabled port.

**efm-oam port chassis/slot/port[-port2] hello-interval seconds**

**Syntax Definitions**

- **chassis**
  - The chassis identifier.
- **slot/port**
  - The slot number for the module and the physical port number on that module.
- **-port2**
  - Specifies the last port in the range of ports.
- **seconds**
  - Specifies the time interval (in seconds) this port waits before sending out the next hello packet. The range for this timer is 1 to 60 seconds.

**Defaults**

By default, the hello-interval value is set to 1 second.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the hello-interval value of 1 second to reset the timer to its default value.
- On a given port, hello interval time period should not be more than half of keep alive timer on the peer port.

**Examples**

-> efm-oam port 1/1/1 hello-interval 5
-> efm-oam port 2/1/1-10 hello-interval 10

**Release History**

Release 8.5R4; command was introduced.
Related Commands

**efm-oam port hello-interval**
Configures the time interval (in seconds) by which the information OAMPDUs are transmitted out of a LINK OAM enabled port.

**efm-oam port keepalive-interval**
Configures the timeout interval for the dynamically learned neighboring devices on a port or on a range of ports. Keepalive-interval is the maximum time period for which a LINK OAM port shall wait for a hello message from its peer before resetting a discovery session.

**show efm-oam port detail**
Displays the configuration and other related parameters for a port.

MIB Objects

alaDot3OamTable
  alaDot3OamHelloInterval
efm-oam port remote-loopback

Specifies whether loopback requests from peers are processed or ignored on the specified port.

```
efm-oam port chassis/slot/port[-port2] remote-loopback {process | ignore}
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot number for the module and the physical port number on that module.
- **-port2**: Specifies the last port in the range of ports.
- **process**: Processes incoming loopback request from peer LINK OAM port.
- **ignore**: Ignore (discard) incoming loopback requests.

### Defaults

By default, the incoming loopback requests are ignored.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900X48C6/T48C6</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900X48C4E/V48C8</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900C32E/T24C2</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900X24C2</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When the remote-loopback is in **process** mode, the session started by peer LINK OAM client will be processed by local LINK OAM port. As a result, remote port will be in remote-loopback state and the local port will be local-loopback state.
- When the remote-loopback is in **ignore** mode, the session started by peer LINK OAM will not be processed by the local port.

### Examples

```
- efm-oam port 1/1/1 remote-loopback process
- efm-oam port 1/1/1 remote-loopback ignore
- efm-oam port 2/1/1-10 remote-loopback process
- efm-oam port 2/1/1-4 remote-loopback ignore
```

### Release History

Release 8.5R4; command was introduced.
Related Commands

**efm-oam port remote-loopback start**
Initiates the loopback control PDU towards the peer port to start or stop the loopback session on the specified port.

**show efm-oam port detail**
Displays the LINK OAM configuration and other related parameters for a port.

**show efm-oam port remote detail**
Displays the configuration and details of the related parameters of the remote port.

MIB Objects

**dot3OamLoopbackTable**

**dot3OamLoopbackIgnoreRx**
efm-oam port remote-loopback start

Initiates the loopback control PDU towards the peer port to start or stop the loopback session on the specified port.

\[
\text{efm-oam port chassis/slot/port remote-loopback \{start | stop\}}
\]

**Syntax Definitions**

- **chassis**
  - The chassis identifier.
- **slot/port**
  - The slot number for the module and the physical port number on that module.
- **start**
  - Specifies whether to start the loopback request.
- **stop**
  - Specifies whether to stop the loopback request.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Before issuing this command, the LINK OAM port has to be in active mode and discovery of peer ports has to be completed.
- When loopback is started from a port towards a peer port which is configured to ignore the loopback request, the loopback response timer will timeout and no error is displayed. In such case, verify the loopback-state of two ports by using the command **show efm-oam port remote detail**.
- The maximum number of simultaneous loopback sessions supported per network interface is 2. If a third loopback is started through CLI, an error will be displayed at the CLI prompt.

**Examples**

- `-> efm-oam port 1/1/1 remote-loopback start`
- `-> efm-oam port 1/1/1 remote-loopback stop`

**Release History**

Release 8.5R4; command was introduced.
Related Commands

**efm-oam port remote-loopback**  Specifies an action that should perform when a loopback request is received from the peer on a port or on a range of ports.

**show efm-oam port remote detail**  Displays the configuration and details of the related parameters of the remote port.

**show efm-oam configuration**  Displays the global LINK OAM configuration.

MIB Objects

dot3OamLoopbackTable
  
dot3OamLoopbackStatus
efm-oam port propagate-events

Configures whether or not the specified port or range of ports will propagate local event notifications to the remote peer.

`efm-oam port chassis/slot/port[-port2] propagate-events {critical-event | dying-gasp} {enable | disable}`

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port`: The slot number for the module and the physical port number on that module.
- `-port2`: Specifies the last port in the range of ports.
- `critical-event`: Configures the notification status for critical events.
- `dying-gasp`: Configures the notification status for dying gasp events.
- `enable`: Enables the notification of critical-event or dying-gasp events to the peer.
- `disable`: Disables the notification of critical-event or dying-gasp events to the peer.

**Defaults**

By default, the notification status for both critical-event and dying-gasp events is set to enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When the system is set for critical event or a dying-gasp event, the local OAM entity indicates the event through the OAMPDU flags to its peer OAM entity.
- In case of port admin down, the OAM IFU-PDU with dying-gasp bit set will be sent to peer as soon as a failure is detected and transmission will continue till the specific port actually goes down.
- In case of takeover or reload of the switch, the OAM IFU-PDU with dying-gasp bit set will be sent to peer as soon as a failure is detected and transmission will continue till the specific device actually goes down.
- The information PDUs with dying gasp bit set is transmitted towards peer as soon as link-down is detected at NI. However, if there is a link flap (i.e link comes again) before the expiry of link-flap.
timer, then normal information PDU transmission with dying-gasp bit reset shall resume. This will cause clearing of alarms or trap on the peer port.

**Examples**

- `-> efm-oam port 1/1/1 propagate-events critical-event enable`
- `-> efm-oam port 1/1/1 propagate-events critical-event disable`
- `-> efm-oam port 2/1/1-10 propagate-events dying-gasp enable`
- `-> efm-oam port 2/1-4 propagate-events dying-gasp disable`

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- `show efm-oam port remote detail` Displays the configuration and details of the related parameters of the remote port.
- `show efm-oam port statistics` Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

**MIB Objects**

- `dot3OamEventConfigTable`
  - `dot3OamDyingGaspEnable`
  - `dot3OamCriticalEventEnable`
**efm-oam errored-frame-period**

Configures the threshold, window frame values and the status for notification when the number of frame-errors exceed the threshold in a given period of time (specified) by window. When the number of frame errors exceeds a threshold within a given window defined by a number of frames (for example, 10 frames out of 1000 had errors), an Errored Frame Period event is generated.

```
efm-oam port chassis/slot/port[-port2] errored-frame-period [threshold threshold_symbols] [window window_frames] [notify {enable | disable}]
```

**Syntax Definitions**

- **chassis**
  The chassis identifier.

- **slot/port**
  The slot number for the module and the physical port number on that module.

- **-port2**
  The last port number in a range of ports that you want to configure on the same slot.

- **threshold_symbols**
  Specifies the frame error threshold number. The range supported is 1 to maximum 4 byte integer value (4294967295).

- **window_frames**
  Specifies the number of frames used to define a window within which the frame period errors are measured.

- **enable**
  Enables notification of the Errored Frame Period event.

- **disable**
  Disables notification of the Errored Frame Period event.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold_symbols</td>
<td>1 frame error</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

The default for window_frames depends on the port-types. The default, minimum and maximum supported values for various port-types are:

<table>
<thead>
<tr>
<th>port-type</th>
<th>default value</th>
<th>minimum value</th>
<th>maximum value</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 mbps</td>
<td>200000</td>
<td>20000</td>
<td>120000000</td>
</tr>
<tr>
<td>1000 X</td>
<td>20000000</td>
<td>2000000</td>
<td>1200000000</td>
</tr>
<tr>
<td>1000 T</td>
<td>20000000</td>
<td>2000000</td>
<td>1200000000</td>
</tr>
<tr>
<td>10 Gig</td>
<td>200000000</td>
<td>200000000</td>
<td>12000000000</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The command can be issued in any order like window, threshold, and notify. However, at least one option needs to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).

Examples

```plaintext
-> efm-oam port 1/1/1 errored-frame-period threshold 1 window 3000000 notify enable
-> efm-oam port 1/1/1 errored-frame-period notify disable
-> efm-oam port 2/1/1-4 errored-frame-period threshold 1 window 3000000 notify enable
-> efm-oam port 2/1/1-2 errored-frame-period notify disable
```

Release History

Release 8.5R4; command was introduced.

Related Commands

- `efm-oam errored-frame`: Configures the threshold, window and notify-status for errored-frame on a port. The frame-period measures the frame-errors, within a specified window of time.
- `efm-oam errored-frame-seconds-summary`: Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port. The Errored Seconds are the time in seconds in which at least one frame error has occurred.
- `show efm-oam port detail`: Displays the Errored Frame Period Event threshold, window, and notification parameter values for a port.

MIB Objects

- `dot3OamEventConfigTable`
- `dot3OamErrFramePeriodWindow`
- `dot3OamErrFramePeriodThreshold`
- `dot3OamErrFramePeriodEvNotifEnable`
**efm-oam errored-frame**

Configures an error frame threshold or window on a LINK OAM port and set notification status for errored frame events. When the number of frame errors exceeds a threshold within a given window defined by a period of time (for example, 10 frames in 1 second had errors), an Errored Frame Event is generated.

```
efm-oam port chassis/slot/port[-port2] errored-frame [threshold threshold_symbols] [window window_seconds] [notify {enable | disable}]
```

### Syntax Definitions

- `chassis` The chassis identifier.
- `slot/port` The slot number for the module and the physical port number on that module.
- `port2` The last port number in a range of ports that you want to configure on the same slot.
- `threshold_symbols` Specifies the frame error threshold number.
- `window_seconds` Specifies the window of time, in which the frame errors will be measured. The duration should be in units of 100ms.
- `enable` Enables notification of the Errored Frame event.
- `disable` Disables notification of the Errored Frame event.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold_symbols</td>
<td>1 frame error</td>
</tr>
<tr>
<td>window_seconds</td>
<td>1 second (10 dsec)</td>
</tr>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
<tr>
<td>disable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The various options, threshold, window and notify can be issued in any order. However, at least one option has to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).
**Examples**

-> efm-oam port 1/1/1 errored-frame threshold 10 window 32 notify enable
-> efm-oam port 1/1/1 errored-frame notify disable
-> efm-oam port 2/1/1-4 errored-frame threshold 10 window 32 notify enable
-> efm-oam port 2/1/1-2 errored-frame notify disable

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- **efm-oam errored-frame-seCONDS-summARY**
  Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port.

- **efm-oam errored-frame-period**
  Configures the threshold, window and notify-status for errored-frame-period errors on a port. The errored-frame-period measures the frame-errors, within a specified window of frames.

- **show efm-oam port statistics**
  Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

**MIB Objects**

dot3OamEventConfigTable
  dot3OamErrFrameWindow
  dot3OamErrFrameThreshold
  dot3OamErrFrameEvNotifEnable
efm-oam errored-frame-seconds-summary

Configures the threshold, window and notify-status for errored-frame-seconds-summary on a port. The Errored Seconds are the time in seconds in which at least one frame error has occurred.

`efm-oam port chassis/slot/port[-port2] errored-frame-seconds-summary [threshold threshold_seconds] [window window_seconds] [notify {enable | disable}]`

**Syntax Definitions**

- `chassis`: The chassis identifier.
- `slot/port`: The slot number for the module and the physical port number on that module.
- `-port2`: The last port number in a range of ports that you want to configure on the same slot.
- `threshold_symbols`: Specifies the frame error threshold number.
- `window_seconds`: Specifies the window of time in which the frame errors will be measured.
- `enable`: Enables notification of the Errored Frame Seconds Summary event.
- `disable`: Disables notification of the Errored Frame Seconds Summary event.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>threshold_symbols</code></td>
<td>1 errored frame second</td>
</tr>
<tr>
<td><code>window_seconds</code></td>
<td>60 seconds. (600 dsec).</td>
</tr>
<tr>
<td>`enable</td>
<td>disable`</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The various options, threshold, window and notify can be issued in any order. However, at least one option has to be entered.
- To enter many ports in a single command, use a hyphen to specify a range of ports (e.g. 3/1-16).
**Examples**

-> efm-oam port 1/1/1 errored-frame-seconds-summary threshold 1 window 700 notify enable
-> efm-oam port 1/1/1 errored-frame-seconds-summary notify disable
-> efm-oam port 2/1/1-4 errored-frame-seconds-summary threshold 1 window 700 notify enable
-> efm-oam port 2/1/1-2 errored-frame-seconds-summary notify disable

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- **efm-oam errored-frame** Configures the threshold, window and notify-status for errored-frame on a port. The frame-period measures the frame-errors, within a specified window of time.

- **efm-oam errored-frame-period** Configures the threshold, window and notify-status for errored-frame-period errors on a port. The errored-frame-period measures the frame-errors, within a specified window of frames.

- **show efm-oam port statistics** Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

**MIB Objects**

- dot3OamEventConfigTable
- dot3OamErrFrameSecsSummaryWindow
- dot3OamErrFrameSecsSummaryThreshold
- dot3OamErrFrameSecsEvNotifEnable
efm-oam multiple-pdu-count

Configures the value of multiple PDU count. When multiple PDU count is set to a specific number in case of any of the threshold cross events, the same event notification PDU will be transmitted that many times towards the peer.

```plaintext
efm-oam multiple-pdu-count count
```

### Syntax Definitions

`count` Specifies the number of PDUs that have to be sent in case of event-notification TLVs. The range is 1 to 10 PDUs.

### Defaults

By default, the PDU-count value is set to 3.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```plaintext
-> efm-oam multiple-pdu-count 5
```

### Release History

Release 8.5R4; command was introduced.

### Related Commands

- `show efm-oam configuration` Displays the global LINK OAM configuration.
- `show efm-oam port remote detail` Displays the configuration and details of the related parameters of the remote port.

### MIB Objects

- `alaDot3OamMultiplePduCount`
**efm-oam port l1-ping**

Configures the number of frames to be sent by the current LINK OAM port to the remote port’s MAC address (l1 ping) and the delay between each consecutive sent frames and to start the ping operation.

```
efm-oam port chassis/slot/port l1-ping [num-frames number] [delay milliseconds] [start]
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot/port**: Specifies the slot number for the module and the physical port number on that module.
- **number**: Specifies the number of frames that needs to be sent during ping operation. The allowed range of numbers is between 1 to 20.
- **milliseconds**: Specifies time interval between two consecutive PDUs. The allowed range of delay is between 100 to 1000 milliseconds.
- **start**: Specifies to start the ping operation.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>5 frames</td>
</tr>
<tr>
<td>milliseconds</td>
<td>1000 milliseconds</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The command is valid only when the LINK OAM is enabled globally, port is in active mode, discovery is done, and the port is in remote loopback mode.
- L1 ping can be started only when the port is in remote loopback mode.

**Examples**

```
-> efm-oam port 1/1/12 l1-ping num-frames 6 delay 300 start
-> efm-oam port 1/1/20 l1-ping num-frames 12 delay 500 start
-> efm-oam port 1/1/15 l1-ping num-frames 5 delay 100 start
-> efm-oam port 1/1/15 l1-ping num-frames 4 delay 200 start
-> efm-oam port 1/1/5 l1-ping num-frames 100 delay 300 start
```
**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- `show efm-oam port l1-ping detail` Displays the frames lost during a loopback session.
- `show efm-oam port statistics` Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

**MIB Objects**

- `alaDot3OamLoopbackTable`  
  - `alaDot3OamPortL1PingFramesConf`  
  - `alaDot3OamPortL1PingFramesDelay`  
  - `alaDot3OamPortL1PingStatus`  
  - `alaDot3OamPortL1PingFramesSent`  
  - `alaDot3OamPortL1PingFramesReceived`  
  - `alaDot3OamPortL1PingAverageRoundTripDelay`
show efm-oam configuration

Displays the global LINK OAM configuration.

Syntax Definitions

N/A

Defaults

N/A.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to display the global configuration of LINK OAM.

Examples

`-> show efm-oam configuration`

EFM OAM Status : enabled,
Multiple PDU Count : 5

Output fields are described here:

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EFM OAM status</td>
<td>The current administrative status of LINK OAM on this switch (Enabled or Disabled).</td>
</tr>
<tr>
<td>Multiple PDU Count</td>
<td>The number of PDUs sent when LINK OAM needs to send multiple Event Notification.</td>
</tr>
</tbody>
</table>

Release History

Release 8.5R4; command was introduced.
Related Commands

**efm-oam admin-state**
Enables or disables the LINK OAM protocol on the switch.

**show efm-oam port detail**
Displays the LINK OAM configuration and other related parameters for a port.

MIB Objects

alaDot3OamStatus
alaDot3OamMultiplePduCount
show efm-oam port

Displays the status of LINK OAM on all the ports in the system, along with other relevant information such as OAM mode, operational status and loopback status of the port.

**show efm-oam port [chassis/slot/port1-port2] [enable | disable] [active | passive]**

---

**Syntax Definitions**

- **chassis**
  - The chassis identifier.

- **slot/port1**
  - The slot number for the module and the physical port number on that module.

- **-port2**
  - The last port number in a range of ports that you want to configure on the same slot (e.g. 3/1-4 specifies ports 1,2,3, and 4 on slot 3).

- **enable**
  - Specifies whether to display the LINK OAM enabled ports.

- **disable**
  - Specifies whether to display the LINK OAM disabled ports.

- **active**
  - Specifies whether to display the LINK OAM active ports.

- **passive**
  - Specifies whether to display the LINK OAM passive ports.

---

**Defaults**

By default, displays the LINK OAM status on all ports.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Use this command to display the state of LINK OAM on the basis of enabled or disabled port and on the basis of active or passive port.

---

**Examples**

```
-> show efm-oam port
Port  EFM-OAM Status  Mode         Operational Status  Loopback Status
---------------+------------+----------------+-------------------+-----------------+---------------------+----------------+-------------------+-----------------+----------------------+
 1/1/1          enabled    active     operational           remoteLoopback
 1/1/2         disabled    active     activeSendLocal       noLoopback
 1/1/3          enabled   passive     activeSendLocal       noLoopback
 1/1/4         disabled    active     activeSendLocal       noLoopback
 1/1/5         disabled    active     activeSendLocal       noLoopback
 1/1/6         disabled    active     activeSendLocal       noLoopback
 1/1/7         disabled    active     activeSendLocal       noLoopback
```
-> show efm-oam port 1/1-5

<table>
<thead>
<tr>
<th>Port</th>
<th>EFM-OAM Status</th>
<th>Mode</th>
<th>Operational Status</th>
<th>Loopback Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>enabled</td>
<td>active</td>
<td>operational</td>
<td>remoteLoopback</td>
</tr>
<tr>
<td>1/1/2</td>
<td>disabled</td>
<td>active</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/3</td>
<td>enabled</td>
<td>passive</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/4</td>
<td>disabled</td>
<td>active</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/5</td>
<td>disabled</td>
<td>active</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
</tbody>
</table>

-> show efm-oam port 1/1-3 enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Operational Status</th>
<th>Loopback Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>active</td>
<td>operational</td>
<td>remoteLoopback</td>
</tr>
<tr>
<td>1/1/3</td>
<td>passive</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
</tbody>
</table>

-> show efm-oam port enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Operational Status</th>
<th>Loopback Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>active</td>
<td>activeSendLocal</td>
<td>remoteLoopback</td>
</tr>
<tr>
<td>1/1/3</td>
<td>passive</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/7</td>
<td>passive</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
</tbody>
</table>

-> show efm-oam port disabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>Operational Status</th>
<th>Loopback Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/2</td>
<td>active</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/4</td>
<td>passive</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/5</td>
<td>active</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
</tbody>
</table>

-> show efm-oam port enabled passive

<table>
<thead>
<tr>
<th>Port</th>
<th>Operational Status</th>
<th>Loopback Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/3</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/7</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
</tbody>
</table>

-> show efm-oam port active

<table>
<thead>
<tr>
<th>Port</th>
<th>EFM-OAM Status</th>
<th>Operational Status</th>
<th>Loopback Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>enabled</td>
<td>activeSendLocal</td>
<td>remoteLoopback</td>
</tr>
<tr>
<td>1/1/2</td>
<td>disabled</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/3</td>
<td>enabled</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/4</td>
<td>enabled</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/5</td>
<td>disabled</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/6</td>
<td>disabled</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
<tr>
<td>1/1/7</td>
<td>disabled</td>
<td>activeSendLocal</td>
<td>noLoopback</td>
</tr>
</tbody>
</table>

**output definitions**

- **Port**: Displays the chassis/slot/port number.
- **EFM-OAM Status**: The state of the EFM-OAM. LINK OAM instance can have any of the following status.
  - **Enabled**: Specifies that the LINK OAM is disabled on the interface.
  - **Disabled**: Specifies that the LINK OAM is disabled on the interface.
**Output Definitions (continued)**

**Operational Status**

The status of the port in discovering whether the peer has LINK OAM capability or not. It has the following states:

- **activeSendLocal**: Specifies that the LINK OAM port is actively trying to discover whether the peer has LINK OAM capability but has not yet made that determination.

- **sendLocalAndRemote**: Specifies that the local LINK OAM port has discovered the peer but has not yet accepted or rejected the configuration of the peer. The local device will then decide that the peer device is acceptable or unacceptable and then accept or decline LINK OAM peering.

- **sendLocalAndRemoteOk**: Specifies the state when LINK OAM peering is allowed by the local port.

- **oamPeeringLocallyRejected**: Specifies the state when the local OAM entity rejects the peer OAM entity.

- **oamPeeringRemotelyRejected**: Specifies the state when the remote LINK OAM port rejects the peering.

- **operational**: Specifies the state when the local LINK OAM port learns that both the local LINK OAM entity and the remote LINK OAM entity have accepted the peering.

- **nonOperHalfDuplex**: Specifies the value nonOperHalfDuplex is returned whenever LINK OAM is enabled. Since LINK OAM functions are not designed to work completely over half-duplex interfaces, the value nonOperHalfDuplex is returned whenever LINK OAM is enabled but the interface is in half-duplex operation.

- **linkFault**: Specifies that the link between the host and the peer has detected a fault.

- **passiveWait**: Specifies that the LINK OAM ports are in passive mode.

**Loopback Status**

The state of remote loopback. It can be **initiatingLoopback**, **terminatingLoopback**, **localLoopback**, **remoteLoopback**, **noLoopback**, or **unknown**.

**Mode**

The state of LINK OAM mode, **active** or **passive**.

**Release History**

Release 8.5R4; command was introduced.
**Related Commands**

*efm-oam multiple-pdu-count*  
Configures the value of multiple PDU count. When multiple PDU count is set to a specific number in case of any of the threshold cross events, the same event notification PDU will be transmitted that many times towards the peer.

**MIB Objects**

dot3OamTable  
dot3OamAdminState  
dot3OamMode  
dot3OamOperStatus  
dot3OamLoopbackTable  
dot3OamLoopbackStatus
**show efm-oam port detail**

Displays the LINK OAM configuration and other related parameters for a port.

```
show efm-oam port chassis/slot/port detail
```

### Syntax Definitions

- `chassis`  
The chassis identifier.
- `slot/port`  
The slot number for the module and the physical port number on that module.

### Defaults

N/A.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8</th>
<th>6900C32E/T24C2</th>
<th>6900X24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use this command when you want to get LINK OAM configuration details for a specific port.

### Examples

```
-> show efm-oam port 1/1/1 detail
OAM Status                   : enable,
Operational Status           : activeSendLocal,
Mode                         : active,
Max OamPDU size              : 1518,
Config Revision              : 0,
Functions Supported          : loopback,event notification,
Loopback Status              : noLoopback,
Loopback Rx Status           : ignore,
Max OamPDUs                  : 10,
KeepAlive Interval(seconds)  : 10,
Hello Interval(seconds)      : 5,
Dying Gasp Notify Status     : enable,
Critical Event Notify Status : enable

Link Monitoring             Window      Threshold  Notify
------------------+------------+-------------+------------+---------------
errored-frame                   10 dsec    10 frames       enable
errored-frame-period            2000000 frames     10 frames       enable
errored-frame-seconds-summary   600 dsec    1 framesec      enable
```
**output definitions**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAM Status</td>
<td>The state of LINK OAM on the port.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The state of the port in discovering whether the peer has LINK OAM capability or not.</td>
</tr>
<tr>
<td>Mode</td>
<td>The state of LINK OAM mode on the port, <strong>active</strong> or <strong>passive</strong>.</td>
</tr>
<tr>
<td>Max OampDU size</td>
<td>Displays the maximum OAMPDU that the LINK OAM port can support.</td>
</tr>
<tr>
<td>Config Revision</td>
<td>Displays the configuration revision of the LINK OAM port as reflected in the latest OAMPDU sent by the peer port.</td>
</tr>
<tr>
<td>Functions Supported</td>
<td>Displays the LINK OAM functions supported by the specified port.</td>
</tr>
<tr>
<td>Loopback Status</td>
<td>Displays the loopback status of the specified LINK OAM port.</td>
</tr>
<tr>
<td>Loopback Rx Status</td>
<td>The action that should be performed by the LINK OAM port when a loopback request is received from the peer port.</td>
</tr>
<tr>
<td>Max OamPDUs</td>
<td>Specifies the maximum OAMPDUs that can be exchanged between two peers.</td>
</tr>
<tr>
<td>KeepAlive Interval</td>
<td>Displays the timeout interval of the specified LINK OAM port for the dynamically learned peer port.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Displays the time interval between two OAMPDUs in seconds.</td>
</tr>
<tr>
<td>Dying Gasp Notify Status</td>
<td>The state of notification for dying gasp events, <strong>enable</strong> or <strong>disable</strong>.</td>
</tr>
<tr>
<td>Critical Event Notify Status</td>
<td>The state of notification for critical events, <strong>enable</strong> or <strong>disable</strong>.</td>
</tr>
<tr>
<td>Link Monitoring</td>
<td>Displays the errors detected on the remote link.</td>
</tr>
<tr>
<td>Window</td>
<td>The frame error event window in the received OAMPDU.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of errored frames in the period required for the event to be generated.</td>
</tr>
<tr>
<td>Notify Status</td>
<td>The state of notification for LINK OAM errors on the port, <strong>enable</strong> or <strong>disable</strong>.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

**show efm-oam port** Displays the status of LINK OAM on all the ports in the system, along with other relevant information like OAM mode, operational status and loopback status of the port.
**MIB Objects**

`dot3OamTable`
- `dot3OamAdminState`
- `dot3OamOperStatus`
- `dot3OamMode`
- `dot3OamMaxOamPduSize`
- `dot3OamConfigRevision`
- `dot3OamFunctionsSupported`

`alaDot3OamTable`
- `alaDot3OamKeepAliveInterval`
- `alaDot3OamHelloInterval`

`dot3OamLoopbackTable`
- `dot3OamLoopbackStatus`
- `dot3OamLoopbackIgnoreRx`

`dot3OamEventConfigTable`
- `dot3OamDyingGaspEnable`
- `dot3OamCriticalEventEnable`
- `dot3OamErrFramePeriodWindow`
- `dot3OamErrFramePeriodThreshold`
- `dot3OamErrFramePeriodEvNotifEnable`
- `dot3OamErrFrameWindow`
- `dot3OamErrFrameThreshold`
- `dot3OamErrFrameEvNotifEnable`
- `dot3OamErrFrameSecsSummaryWindow`
- `dot3OamErrFrameSecsSummaryThreshold`
- `dot3OamErrFrameSecsEvNotifEnable`
show efm-oam port statistics

Displays the LINK OAM statistics on a port, or a range of ports or on all ports.

show efm-oam port chassis/slot/port[-port2] statistics

show efm-oam port statistics

Syntax Definitions

chassis
  The chassis identifier.

slot/port
  Specifies the slot number for the module and the physical port number on that module.

-port2
  The last port number in a range of ports that you want to configure on the same slot.

Defaults

By default, the statistics of all ports are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the port parameter to display the statistics of a specific port.

Examples

-> show efm-oam port 1/1/1 statistics
Port 1/1/1:
  Information OAMPDU Tx : 1035,
  Information OAMPDU Rx : 988,
  Unique Event Notification OAMPDU Tx : 0,
  Unique Event Notification OAMPDU Rx : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx : 1,
  Loopback Control OAMPDU Rx : 0,
  Unsupported OAMPDU Tx : 0,
  Unsupported OAMPDU Rx : 0,
  Frames Lost due to OAM : 0
-> show efm-oam port 1/1-4 statistics

Port 1/1:
  Information OAMPDU Tx : 1035,
  Information OAMPDU Rx : 988,
  Unique Event Notification OAMPDU Tx : 0,
  Unique Event Notification OAMPDU Rx : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx : 1,
  Loopback Control OAMPDU Rx : 0,
  Unsupported OAMPDU Tx : 0,
  Unsupported OAMPDU Rx : 0,
  Frames Lost due to OAM : 0

Port 1/2:
  Information OAMPDU Tx : 1035,
  Information OAMPDU Rx : 988,
  Unique Event Notification OAMPDU Tx : 0,
  Unique Event Notification OAMPDU Rx : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx : 1,
  Loopback Control OAMPDU Rx : 0,
  Unsupported OAMPDU Tx : 0,
  Unsupported OAMPDU Rx : 0,
  Frames Lost due to OAM : 0

Port 1/3:
  Information OAMPDU Tx : 1035,
  Information OAMPDU Rx : 988,
  Unique Event Notification OAMPDU Tx : 0,
  Unique Event Notification OAMPDU Rx : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx : 1,
  Loopback Control OAMPDU Rx : 0,
  Unsupported OAMPDU Tx : 0,
  Unsupported OAMPDU Rx : 0,
  Frames Lost due to OAM : 0

Port 1/4:
  Information OAMPDU Tx : 1035,
  Information OAMPDU Rx : 988,
  Unique Event Notification OAMPDU Tx : 0,
  Unique Event Notification OAMPDU Rx : 0,
  Duplicate Event Notification OAMPDU TX : 0,
  Duplicate Event Notification OAMPDU Rx : 0,
  Loopback Control OAMPDU Tx : 1,
  Loopback Control OAMPDU Rx : 0,
  Unsupported OAMPDU Tx : 0,
  Unsupported OAMPDU Rx : 0,
  Frames Lost due to OAM : 0
-> show efm-oam statistics

Port 1/1:
Information OAMPDU Tx : 1035,
Information OAMPDU Rx : 988,
Unique Event Notification OAMPDU Tx : 0,
Unique Event Notification OAMPDU Rx : 0,
Duplicate Event Notification OAMPDU TX : 0,
Duplicate Event Notification OAMPDU Rx : 0,
Loopback Control OAMPDU Tx : 1,
Loopback Control OAMPDU Rx : 0,
Unsupported OAMPDU Tx : 0,
Unsupported OAMPDU Rx : 0,
Frames Lost due to OAM : 0

Port 1/2:
Information OAMPDU Tx : 1035,
Information OAMPDU Rx : 988,
Unique Event Notification OAMPDU Tx : 0,
Unique Event Notification OAMPDU Rx : 0,
Duplicate Event Notification OAMPDU TX : 0,
Duplicate Event Notification OAMPDU Rx : 0,
Loopback Control OAMPDU Tx : 1,
Loopback Control OAMPDU Rx : 0,
Unsupported OAMPDU Tx : 0,
Unsupported OAMPDU Rx : 0,
Frames Lost due to OAM : 0

Port 1/3:
Information OAMPDU Tx : 1035,
Information OAMPDU Rx : 988,
Unique Event Notification OAMPDU Tx : 0,
Unique Event Notification OAMPDU Rx : 0,
Duplicate Event Notification OAMPDU TX : 0,
Duplicate Event Notification OAMPDU Rx : 0,
Loopback Control OAMPDU Tx : 1,
Loopback Control OAMPDU Rx : 0,
Unsupported OAMPDU Tx : 0,
Unsupported OAMPDU Rx : 0,
Frames Lost due to OAM : 0

output definitions

<table>
<thead>
<tr>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information OAMPDU Tx</td>
<td>The number of OAM PDUs transmitted by the port.</td>
</tr>
<tr>
<td>Information OAMPDU Rx</td>
<td>The number of OAM PDUs received by the port.</td>
</tr>
<tr>
<td>Unique Event Notification OAMPDU Tx</td>
<td>The number of unique event notification OAM PDUs transmitted by the port.</td>
</tr>
<tr>
<td>Unique Event Notification OAMPDU Rx</td>
<td>The number of unique event notification OAM PDUs received by the port.</td>
</tr>
<tr>
<td>Duplicate Event Notification OAMPDU TX</td>
<td>The number of duplicate event notification OAM PDUs transmitted by the port.</td>
</tr>
<tr>
<td>Duplicate Event Notification OAMPDU Rx</td>
<td>The number of duplicate event notification OAM PDUs received by the port.</td>
</tr>
<tr>
<td>Unsupported OAMPDU Tx</td>
<td>The number of unsupported OAM PDUs transmitted by the port.</td>
</tr>
<tr>
<td>Unsupported OAMPDU Rx</td>
<td>The number of unsupported OAM PDUs received by the port.</td>
</tr>
<tr>
<td>Frames Lost due to OAM</td>
<td>The number of frames discarded by the OAM port.</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- **show efm-oam port history**  
  Displays the log of events that have occurred on a port. This command can also be used to display specific event logs on a port.

**MIB Objects**

- `dot3amStatsTable`
  - `dot3amInformationTx`
  - `dot3amInformationRx`
  - `dot3amUniqueEventNotificationTx`
  - `dot3amUniqueEventNotificationRx`
  - `dot3amDuplicateEventNotificationTx`
  - `dot3amDuplicateEventNotificationRx`
  - `dot3amLoopbackControlTx`
  - `dot3amLoopbackControlRx`
  - `dot3amUnsupportedCodesTx`
  - `dot3amUnsupportedCodesRx`
  - `dot3amFramesLostDueToOam`
**show efm-oam port remote detail**

Displays the LINK OAM configuration and details of the related parameters of the remote port.

`show efm-oam port chassis/slot/port remote detail`

---

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port**
  - Specifies the slot number for the module and the physical port number on that module.

---

### Defaults

N/A.

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

N/A.

---

### Examples

```
-> show efm-oam port 1/1/1 remote detail
Remote MAC address : 00:30:96:fd:6b:fa,
Remote Vendor (info): 0x15a1
Remote Vendor (oui) : XYZ
Mode : active,
Max OAMPDU size : 1518,
Config Revision : 0,
Functions Supported : loopbackSupportEventSupport
```

**output definitions**

- **Remote MAC address**
  - Displays the MAC address of the remote peer.

- **Remote Vendor (info)**
  - Displays the vendor number in hexadecimal of the remote peer.

- **Remote Vendor (oui)**
  - Displays the Organizationally Unique Identifier (OUI) number of the remote peer.

- **Mode**
  - The state of LINK OAM mode on the remote port, **active** or **passive**.

- **Max OAMPDU size**
  - Displays the maximum OAMPDU size that the remote LINK OAM port can support.
### Output Definitions (continued)

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Config Revision</strong></td>
<td>Displays the configuration revision of the remote LINK OAM port.</td>
</tr>
<tr>
<td><strong>Functions Supported</strong></td>
<td>Displays the LINK OAM functions supported by the remote port.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.5R4; command was introduced.

### Related Commands

**show efm-oam port history**  
Displays the log of events that have occurred on a port. This command can also be used to display specific event logs on a port.

**clear efm-oam statistics**  
Clears the LINK OAM statistics on a port.

### MIB Objects

- `dot3OamPeerTable`
  - `dot3OamPeerMacAddress`
  - `dot3OamPeerVendorOui`
  - `dot3OamPeerVendorInfo`
  - `dot3OamPeerMode`
  - `dot3OamPeerMaxOamPduSize`
  - `dot3OamPeerConfigRevision`
  - `dot3OamPeerFunctionsSupported`
**show efm-oam port history**

Displays the log of events that have occurred on a port. Use this command to display specific event logs on a port.

```
show efm-oam port chassis/slot/port history [log-type { link-fault | errored-frame | errored-frame-period | errored-frame-seconds | dying-gasp | critical}]
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot/port**
  - Specifies the slot number for the module and the physical port number on that module.

- **link-fault**
  - Displays link fault event logs. Specifies the loss of signal is detected by the receiver. This is sent once per second in the Information OAMPDU.

- **errored-frame**
  - Displays errored-frame event log. an errored frame event occurs when the number of detected error frames over a specific interval exceeds the predefined threshold.

- **errored-frame-period**
  - Displays an errored-frame-period event logs. An errored frame period event occurs if the number of frame errors in specific number of received frames exceeds the predefined threshold.

- **errored-frame-seconds**
  - Displays errored-frame-seconds event logs. When the number of error frame seconds detected on a port over a detection interval reaches the error threshold, an errored frame seconds event occurs.

- **dying-gasp**
  - Specifies an unrecoverable condition (e.g., a power failure).

- **critical**
  - Specifies a crucial event that has occurred on the port.

### Defaults

By default, all log types are displayed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

Timestamp will be in following format:

```
DAY MON Date hh:mm:ss yyyy
```
Examples

-> show efm-oam port 1/1/1 history
Legend: Location: * - Remote, # - Local
LogID  TimeStamp                Log Type          Event Total
-------+-------------------------+-------------+-------+----+
*    1     TUE JAN 06 19:44:51 2009   linkFault       1
#    2     TUE JAN 06 19:45:51 2009   erroredFrame    1

-> show efm-oam port 1/1/1 history log-type link-fault
Legend: Location: * - Remote, # - Local
LogID  TimeStamp                     Event Total
-------+---------+---------+------+-----------+
*   1      TUE JAN 06 19:46:51 2009     1
#   2      TUE JAN 06 19:46:51 2009     1

output definitions

LogID  Specifies individual events within the event log.
Timestamp  The value of actual time at the time of the logged event.
Log Type  Specifies the type of event log.
Event Total  Specifies the total number of times one or more of these occurrences have resulted in an Event Notification.

Release History

Release 8.5R4; command was introduced.

Related Commands

show efm-oam port statistics  Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
clear efm-oam log-history  Clears the LINK OAM event logs history on a port.

MIB Objects

dot3OamEventLogTable
  dot3OamEventLogIndex
  dot3OamEventLogTimestamp
  dot3OamEventLogOui
  dot3OamEventLogType
  dot3OamEventLogLocation
  dot3OamEventLogWindowHi
  dot3OamEventLogWindowLo
  dot3OamEventLogThresholdHi
  dot3OamEventLogThresholdLo
  dot3OamEventLogValue
  dot3OamEventLogRunningTotal
  dot3OamEventLogEventTotal
**show efm-oam port l1-ping detail**

Displays the frames lost during a loopback session.

**show efm-oam port chassis/slot/port l1-ping detail**

### Syntax Definitions

- **chassis**
  
  The chassis identifier.

- **slot/port**
  
  Specifies the slot number for the module and the physical port number on that module.

### Defaults

N/A.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The command can also be used even on a port on which LINK OAM is not enabled.

### Examples

```bash
-> show efm-oam port 1/1/1 l1-ping detail
frames configured = 5,
frames delay (msec) = 100,
L1 ping status = Successful,
frames sent = 4,
frames received = 4,
avg delay (msec) = 5

-> show efm-oam port 1/1/4 l1-ping detail
frames configured = 5,
frames delay (msec) = 200,
L1 ping status = Successful,
frames sent = 4,
frames received = 2,
avg delay (msec) = 15
```

### Output Definitions

- **frames configured**
  
  Specifies the number of frames that are sent during L1-ping.

- **delay configured**
  
  Specifies the delay between transmission of two consecutive frames during L1-ping.
**output definitions (continued)**

| L1 ping status | The status of the L1 ping operation. The status can be **Successful**, **Unsuccessful** or **default**. |
| frames sent | Specifies the frames sent during last L1 ping. |
| frames received | Specifies the frames received during last L1 ping. |
| average delay | Specifies the average delay taken by frames during last L1 ping. |

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

**efm-oam port l1-ping**

Configures the number of frames that needs to be sent during L1-ping, the delay between each consecutive sent frames and to start the L1-ping operation.

**MIB Objects**

alaDot3OamLoopbackTable
- alaDot3OamPortL1PingFramesConf
- alaDot3OamPortL1PingFramesDelay
- alaDot3OamPortL1PingStatus
- alaDot3OamPortL1PingFramesSent
- alaDot3OamPortL1PingFramesReceived
- alaDot3OamPortL1PingAverageRoundTripDelay
clear efm-oam statistics

Clears the LINK OAM statistics on a port, range of ports or all ports.

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot/port**: The slot number for the module and the physical port number on that module.
- **-port2**: Specifies the last port in the range of ports.

### Defaults

By default, the statistics are cleared for all the ports if no port is specified in the command.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the port parameter with this command to clear the statistics for a specific port or range of ports.

### Examples

```plaintext
-> clear efm-oam statistics
-> clear efm-oam statistics port 2/1/1-3
```

### Release History

Release 8.5R4; command was introduced.

### Related Commands

- **show efm-oam port statistics**: Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
- **clear efm-oam log-history**: Clears the LINK OAM event logs history on a port.

### MIB Objects

- alaDot3OamGlobalClearStats
- alaDot3OamStatsTable
alaDot3OamPortClearStats
clear efm-oam log-history

Clears the LINK OAM event logs history a port, range of ports or all ports.

`clear efm-oam log-history [port chassis/slot/port[-port2]]`

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot/port` The slot number for the module and the physical port number on that module.
- `-port2` Specifies the last port in the range of ports.

**Defaults**

By default, the event logs are cleared for all the ports if no port is specified in the command.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the port parameter with this command to clear the statistics for a specific port or range of ports.

**Examples**

- `-> clear efm-oam log-history`
- `-> clear efm-oam log-history port 1/1/1`
- `-> clear efm-oam log-history port 2/1/1-3`

**Release History**

Release 8.5R4; command was introduced.

**Related Commands**

- `show efm-oam port statistics` Displays the LINK OAM statistics on a port, or a range of ports or on all ports.
- `show efm-oam port history` Displays the log of events that have occurred on a port. Use this command to display specific event logs on a port.

**MIB Objects**

- `alaDot3OamGlobalClearEventLogs`
- `alaDot3OamEventLogTable`
allaDot3OamPortClearEventLogs
CPE Test Head Commands

The Customer Provider Edge (CPE) Test Head traffic generator and analyzer is a Test-OAM (Operation, Administration, and Maintenance) tool used in the Metro Ethernet Network to validate the customer Service Level Agreements (SLA). This functionality allows the operator to validate the Metro Ethernet Network between customer end points, which is critical when provisioning or troubleshooting network services.

This implementation of CPE Test Head supports unidirectional and bidirectional ingress tests. Traffic is generated at the UNI port as if the traffic was generated from a test head connected to the UNI port. This validates the actual customer SLA by subjecting the test traffic to the ingress QoS defined at the UNI port (Ethernet SAP profile or QoS policy rules for priority and bandwidth control) and the egress QoS defined at the egress NNI port and carrier network.

The CPE test is non-disruptive to traffic running on other UNI ports that are associated with the same SAP profile as the test UNI port. All UNI ports, including CPE test ports, are subject to any SAP profile or QoS configuration associated with the port. This is important to consider when analyzing test results.

The feature provides a multi-stream test capability. The CPE multi-test feature is supported on non-metro switches with metro license. The feature supports a stack containing up to eight switches.

Multi-stream test requires a free port. The port must not be used and not have any configuration. When a multi-stream test starts, the port is made out of service. The port is made operational again and the configuration is retained when the test is stopped.

MIB information for the CPE Test Head commands are:

<table>
<thead>
<tr>
<th>Filename</th>
<th>alcatelIND1testoam.mib</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>ALCATEL-IND1-TEST-OAM-MIB</td>
</tr>
</tbody>
</table>
A summary of available commands is listed here:

<table>
<thead>
<tr>
<th>Single-test</th>
<th>Multi-test</th>
</tr>
</thead>
<tbody>
<tr>
<td>test-oam</td>
<td>test-oam group</td>
</tr>
<tr>
<td>test-oam direction</td>
<td>test-oam group tests</td>
</tr>
<tr>
<td>test-oam src-endpoint dst-endpoint</td>
<td>test-oam group feeder</td>
</tr>
<tr>
<td>test-oam port</td>
<td>test-oam group src-endpoint dst-endpoint</td>
</tr>
<tr>
<td>test-oam vlan test-frame</td>
<td>test-oam group role</td>
</tr>
<tr>
<td>test-oam role</td>
<td>test-oam group port</td>
</tr>
<tr>
<td>test-oam duration rate packet-size</td>
<td>test-oam group direction</td>
</tr>
<tr>
<td>test-oam frame</td>
<td>test-oam group duration rate</td>
</tr>
<tr>
<td>test-oam I2-saa</td>
<td>test-oam group start stop</td>
</tr>
<tr>
<td>test-oam start stop</td>
<td>test-oam group remote-sys-mac</td>
</tr>
<tr>
<td>test-oam statistics flash-logging</td>
<td>show test-oam group</td>
</tr>
<tr>
<td>show test-oam</td>
<td>show test-oam group stats</td>
</tr>
<tr>
<td>show test-oam saa statistics</td>
<td>clear test-oam group stats</td>
</tr>
<tr>
<td>clear test-oam statistics</td>
<td>clear test-oam group stats</td>
</tr>
</tbody>
</table>
test-oam

Configures the CPE test name and an optional description. The test name is used to identify and configure a CPE test profile.

`test-oam` `string [descr description]`

`no test-oam` `string`

**Syntax Definitions**

*`string`* The name of the CPE test, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test and is also referred to as the test ID.

*`description`* The description to assign to the test name, an alphanumeric string between 1 and 32 characters.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>description</code></td>
<td>DEFAULT</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to remove the specified CPE test configuration.
- This command creates a new CPE test profile that is identified by the test name. Make sure the name specified does not exist in the switch configuration.
- A maximum of 32 tests can be configured.
- Only one test can be active on the switch at any given time.

**Examples**

```
-> test-oam Test1
-> test-oam Test2 descr second-test
-> no test-oam Test2
```
**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **show test-oam**
  Displays the CPE test configuration and status.

- **show test-oam statistics**
  Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

**MIB Objects**

- **alaTestOamConfigTable**
  - **alaTestOamConfigTestName**
  - **alaTestOamConfigTestDescription**
  - **alaTestOamConfigRowStatus**
**test-oam direction**

Configures the CPE test direction.

```
test-oam string [direction {unidirectional | bidirectional}]
```

**Syntax Definitions**

- `string` The name of the CPE test, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test and is also referred to as the test ID.

- `direction` The direction of the CPE test.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>unidirectional</td>
<td>unidirectional</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command assigns the direction to the CPE test.

**Examples**

- `-> test-oam Test1 direction unidirectional`
- `-> test-oam Test1 direction bidirectional`

**Release History**

Release 8.6R1; command was introduced.
Related Commands

- **show test-oam**
  Displays the CPE test configuration and status.

- **show test-oam statistics**
  Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

MIB Objects

- **alaTestOamConfigTable**
  - **alaTestOamConfigTestName**
  - **alaTestOamConfigDirection**
**test-oam src-endpoint dst-endpoint**

Configures the source and destination endpoints for the specified test.

`test-oam string [src-endpoint src-string] [dst-endpoint dst-string]`

### Syntax Definitions

**string**

The name of an existing CPE test. The string can be of length 1 to 32 characters.

**src-string**

This represents the local or transmitting device. The management IP address or DNS host name of the switch that will transmit test traffic. In case of bidirectional test this also identifies the analyzer device. The string can be of length 1 to 32 characters.

**dst-string**

This represents the remote device. The management IP address or DNS host name of the switch that will receive test traffic. This is the switch on which traffic analysis is done. For unidirectional test this represents the analyzer device. For bidirectional test this identifies the device on which the loopback mode must be active. The string can be of length 1 to 32 characters.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The endpoint can be set as switch hostname or switch management IP address.
- Using the DNS host name of the switch is highly recommended, as this name is unique and is mapped to an IP address configured for the switch.
- This command automatically overwrites the source and destination endpoint values previously configured for the specified CPE test.
- Multicast and broadcast address must not be configured for bidirectional test.

### Examples

-> `test-oam Test1 src-endpoint SW1 dst-endpoint SW2`

-> `test-oam Test1 src-endpoint SW1`
-> test-oam Test1 dst-endpoint SW2

**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **test-oam port**
  Configures the port on which the CPE test will run.

- **show test-oam**
  Displays the CPE test configuration and status.

**MIB Objects**

- **alaTestOamConfigTable**
  - **alaTestOamConfigTestName**
  - **alaTestOamConfigSourceEndpoint**
  - **alaTestOamConfigDestinationEndpoint**
**test-oam port**

Configures the port on which the CPE test will run. Use this command on the switch that will generate the test traffic. If the switch is going to receive test traffic, configuring a test port is not necessary.

**test-oam string port chassis/slot/port**

---

**Syntax Definitions**

- **string**: The name of an existing CPE test.
- **chassis/slot/port**: The port on which the CPE test will generate traffic.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- In an Ethernet Service environment, the UNI port is designated as the test port on the generator switch to simulate traffic coming in on the port as if it was sent from a test head device. This will subject the test traffic to the SAP profile.

- Note that the customer traffic is disrupted on ports configured as CPE test ports. Configuring a port that is not in use is recommended. In addition, if the test port is a UNI port associated with an SAP profile, only that UNI port is used for the test. Traffic on other UNI ports associated with the same profile is not disrupted by the CPE test.

- All UNI ports, including CPE test ports, are subject to any SAP profile or QoS configuration associated with the port. This must be considered when test results are analyzed.

- This command automatically overwrites the port value previously configured for the specified CPE test.

---

**Examples**

```
-> test-oam Test1 port 1/1/2
```

---

**Release History**

Release 8.6R1; command was introduced.
**Related Commands**

- **test-oam vlan test-frame**  
  Configures the source mac-address, destination mac-address, and the SVLAN for the test-frame used in the test.

- **show test-oam**  
  Displays the CPE test configuration and status.

**MIB Objects**

- **alaTestOamConfigTable**
  - **alaTestOamConfigTestName**
  - **alaTestOamConfigPort**
test-oam vlan test-frame

Configures the SVLAN and the source and destination MAC addresses for the test frame. Use this command to configure these test parameters on both the generator (local) switch and the analyzer (remote) switch for the specified CPE test.

```bash
test-oam string [vlan svlan] [[test-frame [src-mac src-address] [dst-mac dst-address]]
```

Syntax Definitions

- `string`: The name of an existing CPE test.
- `svlan`: The service VLAN ID. This is used for traffic analysis and test-frame accounting.
- `src-address`: Source mac-address of the test-frame.
- `dst-address`: Destination mac-address of the test-frame.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>src-address</td>
<td>00:00:00:00:00:00</td>
</tr>
<tr>
<td>dst-address</td>
<td>00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Although the source and destination MAC addresses are optional parameters with this command, the test will not run if these addresses are set to all zeros (the default).
- Make sure that routing is disabled on the specified SVLAN.
- Avoid configuring any IEEE reserved MAC addresses as the destination MAC address for the test.
- This command automatically overwrites the SVLAN, source MAC, or destination MAC values previously configured for the specified CPE test.

Examples

```bash
-> test-oam Test1 vlan 100 test-frame src-mac 00:01:02:00:00:02 dst-mac 00:00:01:00:00:90
-> test-oam Test1 vlan 100
```
CPE Test Head Commands

test-oam vlan test-frame

-> test-oam Test1 test-frame src-mac 00:01:02:00:00:02 dst-mac 00:00:01:00:00:90
-> test-oam Test1 test-frame src-mac 00:01:02:00:00:02
-> test-oam Test test-frame dst-mac 00:00:01:00:00:90

Release History
Release 8.6R1; command was introduced.

Related Commands
- **test-oam role** Configures the switch as a generator or analyzer for the test.
- **show test-oam** Displays the CPE test configuration and status.

MIB Objects
alaTestOamConfigTable
  alaTestOamConfigTestName
  alaTestOamConfigVlan
  alaTestOamConfigFrameSrcMacAddress
  alaTestOamConfigFrameDstMacAddress
test-oam role

Configures the role the switch will perform for the specified CPE test. The type of role assigned determines whether the switch transmits (generator) or receives (analyzer) or loopback test frames.

test-oam string role {generator | analyzer | loopback}

Syntax Definitions

string The name of an existing CPE test.
generator Configures the switch as the test generator.
analyzer Configures the switch as the test analyzer.
loopback Configures the switch as loopback.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use this command on the switch that will perform the specified role.
- Configuring a generator and an analyzer switch for each test is required.
- Only one role can be assigned to the switch for a particular test.
- This command automatically overwrites the previously configured switch role for the specified CPE test.

Examples

-> test-oam Test1 role generator
-> test-oam Test2 role analyzer
-> test-oam Test2 role loopback

Release History

Release 8.6R1; command was introduced.
Related Commands

test-oam duration rate packet-size
Configures the test frame duration, rate and packet-size for the test.

show test-oam
Displays the CPE test configuration and status.

MIB Objects
alaTestOamConfigTable
  alaTestOamConfigTestName
  alaTestOamConfigRole
test-oam duration rate packet-size

Configures the duration, rate, and packet-size for the specified test. Use this command to configure these test parameters on the generator switch.

```
  test-oam string [duration secs] [rate rate] [packet-size bytes]
```

### Syntax Definitions

- **string**: The name of an existing CPE test.
- **secs**: The duration of the test, in seconds. This is the amount of time the generator will actively transmit test packets to the remote (analyzer) switch. The valid time range is 1–3600 seconds.
- **rate**: The rate, in Kbps or Mbps, at which test traffic is generated. The minimum value allowed is 8 Kbps to line rate. The granularity of the transmit rate is 8 Kbps for 100 Mbps port and 2 Mbps for 1Gig ports.
- **bytes**: The packet size, in bytes. The valid range is 64–9212 bytes.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>secs</td>
<td>5 secs</td>
</tr>
<tr>
<td>rate</td>
<td>8 k</td>
</tr>
<tr>
<td>bytes</td>
<td>64 byte</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command automatically overwrites any duration, rate, and packet size parameter values previously configured for the specified CPE test.
- The status of the CPE test will change to “ended” when the test duration time expires.
- This command automatically overwrites the duration, rate, or packet size values previously configured for the specified CPE test.

### Examples

- `-> test-oam Test1 duration 10 rate 8k packet-size 64`
- `-> test-oam Test1 rate 8m`
-> test-oam Test1 duration 10
-> test-oam Test1 packet-size 64

**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **test-oam frame**
  Configures the test frame parameter values for the CPE test.

- **show test-oam**
  Displays the CPE test configuration and status.

**MIB Objects**

- *alaTestOamConfigTable*
  - *alaTestOamConfigTestName*
  - *alaTestOamConfigDuration*
  - *alaTestOamConfigGeneratorBandwidth*
  - *alaTestOamConfigGeneratorPacketSize*
**test-oam frame**

Configures the test frame parameter values for the specified CPE test. Use this command on the switch that will generate the test frame traffic.

```
test-oam string frame
    [vlan-tag vlan-id priority priority drop-eligible {true | false}]
    ether-type {hex-num | ipv4 {src-ip src-ipv4 dst-ip dst-ipv4 [ttl ttl] [tos tos] [protocol {udp | tcp} {src-port src-port dst-port dst-port}]]] [data-pattern pattern]
```

**Syntax Definitions**

- **string**: The name of an existing CPE test.
- **vlan-id**: The VLAN ID of the frame.
- **priority**: The priority value. The valid range is 0–7.
- **true**: Sets the drop-eligible bit to true.
- **false**: Sets the drop-eligible bit to false.
- **hex-num**: The hexadecimal ethertype value. The valid range is 0x600–0xfffe.
- **src-ipv4**: The source IP address for an IPv4 test frame.
- **dst-ipv4**: The destination IP address for an IPv4 test frame.
- **ttl**: The time-to-live value. The valid range is 0–255.
- **tos**: The type-of-service value for QoS features. The valid range is 0x0–0xff.
- **udp**: Specifies the UDP protocol.
- **tcp**: Specifies the TCP protocol.
- **src-port**: The source port of the generated test frame.
- **dst-port**: The destination port of the generated test frame.
- **pattern**: The data pattern present in the generated test frame. The valid range is 0x0000–0xffff.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>7</td>
</tr>
<tr>
<td>drop-eligible</td>
<td>false</td>
</tr>
<tr>
<td>ttl</td>
<td>64</td>
</tr>
<tr>
<td>tos</td>
<td>0x0</td>
</tr>
<tr>
<td>pattern</td>
<td>0x0000</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Specify the Ether type in hexadecimal format to configure a Layer 2 test frame.
- Specify ipv4 as the Ether type to configure a Layer 3 test frame. When this option is selected, entering a source and destination IP address is required.
- Do not specify reserved Ether type values.
- This command automatically overwrites the test packet parameter values previously configured for the specified CPE test.

Examples

If the ether-type is a hexadecimal number (Layer 2 test frame):
- `-> test-oam Test1 frame vlan-tag 1 priority 2 drop-eligible false ether-type 0x0100 data-pattern 0x0010`

If the ether-type is IPV4 (Layer 3 test frame):
- `-> test-oam Test1 frame vlan-tag 1 priority 2 drop-eligible false ether-type ipv4 src-ip 1.1.1.1 dst-ip 2.2.2.2 ttl 4 tos 0x01 protocol udp src-port 2000 dst-port 3000 data-pattern 0x0010`

Release History

Release 8.6R1; command was introduced.

Related Commands

- `test-oam l2-saa` Start or stop the CPE test.
- `show test-oam` Displays the CPE test configuration and status.

MIB Objects

- `alaTestOamConfigTable`
- `alaTestOamConfigTestName`
- `alaTestOamEtherConfigTable`
- `alaTestOamIpv4ConfigTable`
**test-oam l2-saa**

Configures to run SAA tests in parallel with test streams.

```
test-oam string l2-saa [priority vlan-priority] [count num-pkts] [interval inter-pkt-delay] [continuous] [size size] [drop-eligible {true | false}]
```

```
no test-oam string l2-saa
```

---

**Syntax Definitions**

- **string**: The name of an existing CPE test.
- **vlan-priority**: Specify the internal priority of MAC ping and 802.1p value on the VLAN tag header.
- **num-pkts**: The number of packets sent in one ping iteration. Valid range is 1 to 10.
- **inter-pkt-delay**: The delay between packets sent during a ping iteration (milliseconds). Valid range is 100 to 1000, in multiples of 100.
- **continuous**: Allows the SAA session to run continuously until the test-oam session ends.
- **size**: The payload size to be used for MAC ping iteration. Must be within 1500 bytes.
- **drop-eligible**: Specify the drop precedence of the MAC ping and the Canonical Format Indicator (CFI) bit on the VLAN tag header.

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vlan-priority</strong></td>
<td>0</td>
</tr>
<tr>
<td><strong>num-pkts</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>inter-pkt-delay</strong></td>
<td>1000 ms</td>
</tr>
<tr>
<td><strong>size</strong></td>
<td>36 bytes</td>
</tr>
<tr>
<td><strong>drop-eligible</strong></td>
<td>false</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

- The L2-SAA test derives the source MAC, destination MAC, and the VLAN ID from the test OAM configuration of the individual test frames.
- The default L2-SAA configuration values will be applied if no optional parameters are configured.
- To run the L2-SAA session until the test-oam session ends, use the `continuous` parameter.
- Different SAA profiles can be configured for each individual test stream.
- Use the `no` form of this command to remove the L2-SAA configuration for the test.

Examples

```
-> test-oam test1 12-saa priority 5 count 5 interval 1000 size 100 drop-eligible false
-> test-oam test1 12-saa continuous
-> no test-oam test1 12-saa
```

Release History

Release 8.6R1; command was introduced.

Related Commands

- **test-oam**
  - Configures the CPE test name and an optional description. The test name is used to identify and configure a CPE test profile.
- **show test-oam**
  - Displays the CPE test configuration and status.

MIB Objects

- `alaTestOamConfigTable`
- `alaTestOamSaaConfigDropEligible`
- `alaTestOamSaaConfigPayloadSize`
- `alaTestOamSaaConfigNumPkts`
- `alaTestOamSaaConfigInterPktDelay`
- `alaTestOamSaaContinuous`
**test-oam start stop**

Starts or stops the CPE test operation.

```
test-oam string {{vlan vlan-id} [port chassis/slot/port] [packet-size bytes] start | stop} [fetch-remote-stats]
```

### Syntax Definitions

- **string**
  - The name of an existing CPE test.

- **vlan-id**
  - The service VLAN ID. This value is required only for traffic analysis and test frame accounting and is not related to the VLAN tag specified for the actual test frame.

- **chassis/slot/port**
  - The switch port on which the test is run.

- **bytes**
  - The size of the test packet, in bytes. The valid packet size range is 64–9212 bytes.

- **start**
  - Starts the CPE test operation.

- **stop**
  - Stops the CPE test operation.

- **fetch-remote-stats**
  - Triggers the test at the remote device from the generator. The statistics are collected from the remote device and the test is stopped after receiving the test results.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>64</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Ensure that routing is disabled on the specified service VLAN.

- The optional **vlan**, **port**, and **packet-size** parameters specify “active” parameter values that are applied when the specified CPE test is started. If these same parameters are defined within a CPE test profile, they are considered “configured” parameter values. Active parameter values override configured parameter values when the test is started.
• If no active parameter values are specified with this command, the test is started using the configured values defined in the CPE test profile. However, if active parameter values are not specified and the CPE test does not contain any configured values for these parameters, the test will not run.

• Specifying any of the optional parameter values does not change the configured values associated with the CPE test.

• If the specified port resides on a switch that will transmit test traffic, the port will generate the test frames. However, if the switch is an analyzer switch, specifying a port is not required.

• Start the specified test on the analyzer switch first and then on the generator switch.

• The test will stop when the test duration time expires or when the test is manually stopped using the \texttt{test-oam stop} command.

• Manually restart the test if the test is interrupted by a takeover, restart, or hot swap.

• The previous statistics related to the test will be cleared automatically once the test is started.

• Use the \texttt{fetch-remote-stats} parameter to collect the test statistics from the remote device. This parameter must be used to start the bidirectional test.

\textbf{Examples}

\begin{itemize}
\item \texttt{test-oam Test1 start}
\item \texttt{test-oam Test1 vlan 100 start}
\item \texttt{test-oam Test1 port 1/1/1 start}
\item \texttt{test-oam Test1 packet-size 100 start}
\item \texttt{test-oam Test1 vlan 100 port 1/1/1 packet-size 100 start}
\item \texttt{test-oam Test1 stop}
\item \texttt{test-oam Test1 start fetch-remote-stats}
\item \texttt{test-oam "test2" port 1/1/2 start fetch-remote-stats}
\end{itemize}

\textbf{Release History}

Release 8.6R1; command was introduced.

\textbf{Related Commands}

\begin{itemize}
\item \texttt{show test-oam statistics} \hspace{1em} Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.
\item \texttt{show test-oam} \hspace{1em} Displays the CPE test configuration and status.
\end{itemize}

\textbf{MIB Objects}

\begin{itemize}
\item \texttt{alaTestOamConfigTable}
\item \texttt{alaTestOamConfigTestName}
\item \texttt{alaTestOamConfigVlan}
\item \texttt{alaTestOamConfigPort}
\item \texttt{alaTestOamConfigGeneratorPacketSize}
\item \texttt{alaTestOamConfigTestIdState}
\item \texttt{alaTestOamConfigRemoteStatsFetch}
\end{itemize}
**test-oam remote-sys-mac**

Configures the system MAC address of the remote device to receive test OAM messages.

```
test-oam string remote-sys-mac string
```

### Syntax Definitions

- **string**
  - The name of an existing CPE test.

- **remote-sys-mac**
  - The system MAC address of the remote device.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use this command on the generator switch to set the system MAC address of the remote device to receive the test OAM messages.

- remote-sys-mac must be the primary CMM MAC address of the remote device. Use the `show cmm` command on the remote device to know the chassis MAC address of the device.

- remote-sys-mac is not applicable for analyzer or loopback.

- Configuring the Remote Sys MAC is mandatory for bidirectional test and optional for unidirectional test.

### Examples

```
-> test-oam Test1 remote-sys-mac 00:e0:b1:7c:7a:fa
```

### Release History

Release 8.6R1; command was introduced.
Related Commands

show test-oam

Displays the CPE test configuration and status.

MIB Objects

alaTestOamConfigTable
  alaTestOamConfigRemoteSysMacAddress
test-oam statistics flash-logging

Enable or disable the option to save the statistics of the test on the file in the flash directory of the switch. The test information is appended at the end of the default text file (testoamActiveStats.txt) in the flash.

test-oam statistics flash-logging {enable | disable}

---

**Syntax Definitions**

N/A

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `more` command to read the test results stored on the switch.

**Examples**

- `-> test-oam statistics flash-logging enable`
- `-> test-oam statistics flash-logging disable`

**Release History**

Release 8.6R1; command was introduced.
Related Commands

**show test-oam statistics**  Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

**show test-oam saa statistics**  Clears the statistics for all CPE tests or for a specific test name.

MIB Objects

alaTestOamConfigTable
  alaTestOamConfigStatsSave
show test-oam

Displays the CPE test configuration and status.

**show test-oam [tests | string]**

---

**Syntax Definitions**

tests Displays information for all the CPE tests.
string The name of an existing CPE test.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `tests` parameter to display information for all CPE tests configured on the switch.
- Use the `string` parameter to display detailed information for a specific CPE test.

---

**Examples**

```bash
-> show test-oam tests
Total Test-Ids: 1
Test-Id Port  Src-Mac  Dst-Mac  Vlan  Direction  Status        Remote-Sys-Mac
---------------------------------------------------------------
Test1 none 00:00:00:00:00:00 00:00:00:00:00:00 none unidirectional not-started 00:00:00:00:00:00
```

---

**output definitions**

- **Test-Id** The CPE test name (ID). Configured through the `test-oam` command.
- **Port** The port on which the test is run. Configured through the `test-oam port` command.
- **Src-Mac** The source MAC address of the test frame. Configured through the `test-oam vlan test-frame` command.
- **Dst-Mac** The destination MAC address of the test frame. Configured through the `test-oam vlan test-frame` command.
- **Vlan** The service VLAN (SVLAN) associated with the test. Configured through the `test-oam vlan test-frame` command.
output definitions

<table>
<thead>
<tr>
<th>Direction</th>
<th>The direction of the test traffic. Note that only unidirectional traffic tests are supported.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The operational status of the test.</td>
</tr>
<tr>
<td>Remote-Sys-Mac</td>
<td>The MAC address of the remote device configured through the test-oam remote-sys-mac command.</td>
</tr>
</tbody>
</table>

-> show test-oam Test1
Legend: dei-drop eligible indicator
TEST Parameters for Test1:
  Source Endpoint : SW1,
  Destination Endpoint : SW2,
  Test Description : Ether Test,
  Direction : unidirectional,
  Source MAC : 00:11:22:33:44:55,
  Destination MAC : 00:22:33:44:55:66,
  Remote Sys MAC : E8:E7:32:72:01:A4,
  Duration : 10(secs),
  Vlan : 100,
  Role : generator,
  Port : 1/1,
  Tx Rate : 80m,
  Frame Size : 100,
  State : start,
  Status : running

Frame Configuration:
  Frame Type : ether,
  Vlan : 200,
  Priority : 7,
  Pattern : 0x0001,
  Dei : none,
  Ether Type : 0x8000,

-> show test-oam Test2
TEST Parameters for Test2:
  Source Endpoint : SW1,
  Destination Endpoint : SW2,
  Test Description : IPV6 Test,
  Direction : unidirectional,
  Source MAC : 00:11:22:33:44:55,
  Destination MAC : 00:22:33:44:55:66,
  Remote Sys MAC : E8:E7:32:72:01:A4,
  Duration : 10(secs),
  Vlan : 100,
  Role : generator,
  Port : 1/1,
  Tx Rate : 8k,
  Frame Size : 100,
  State : start,
  Status : running

Frame Configuration:
  Frame Type : ipv6,
  Vlan : 200,
  Priority : 7,
  Pattern : 0x0001,
Dei : true,
Source Ip : 00:00:00:00:10.20.30.50,
Destination Ip : 00:00:00:00:10.30.40.60,
Source Port : 10,
Destination Port : 20,
Next Header : tcp,
Hop-Count : 50,
Traffic-Class : 0xff
Flow-Label : 0x0

L2-SAA Configuration :
L2-SAA DE : False,
L2-SAA Payload Size : 64,
L2-SAA Count : 0,
L2-SAA Interval : 1000,
L2-SAA Continuous : yes
L2-SAA Priority : 0

output definitions
Source Endpoint
The host name for the source (generator) switch. Configured through the test-oam direction command.

Destination Endpoint
The host name for the destination (analyzer) switch. Configured through the test-oam direction command.

Test Description
Description for the test name. Configured through the test-oam command.

Direction
The direction of the test traffic. Note that only unidirectional traffic tests are supported.

Source MAC
The source MAC address for the test frame. Configured through the test-oam vlan test-frame command.

Destination MAC
The destination MAC address for the test frame. Configured through the test-oam vlan test-frame command.

Remote Sys MAC
The MAC address of the remote device configured through the test-oam remote-sys-mac command.

Duration
The amount of time the test will run. Configured through the test-oam duration rate packet-size command.

Vlan
The service VLAN (SVLAN) associated with the test. Configured through the test-oam vlan test-frame command.

Role
The role of the switch for this test (generator or analyzer). Configured through the test-oam role command

Port
The port on which the test is run. Configured through the test-oam port command.

Tx Rate
The rate at which packets are transmitted on the test port. Configured through the test-oam duration rate packet-size command.

Frame Size
The size of the test frame. Configured through the test-oam duration rate packet-size command.

State
The administrative state of the test (stop or start). Configured through the test-oam l2-saa command.

Status
The operational status of the test (running, ended, stopped, or not started).
### Output Definitions

<table>
<thead>
<tr>
<th>Frame Configuration</th>
<th>The test frame type (ether or ipv4) and associated parameter values. Configured through the <code>test-oam frame</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2-SAA Configuration</td>
<td>Displays the L2 SAA configuration.</td>
</tr>
</tbody>
</table>

### Release History

Release 8.6R1; command was introduced.

### Related Commands

**show test-oam statistics**

Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

### MIB Objects

- `alaTestOamConfigTable`
  - `alaTestOamConfigTestId`
  - `alaTestOamConfigPort`
  - `alaTestOamConfigFrameSrcMacAddress`
  - `alaTestOamConfigFrameDstMacAddress`
  - `alaTestOamConfigVlan`
  - `alaTestOamConfigDirection`
  - `alaTestOamConfigTestIdStatus`
  - `alaTestOamConfigRemoteSysMacAddress`

- `alaTestOamSaaConfigTable`
  - `alaTestOamSaaConfigDropEligible`
  - `alaTestOamSaaConfigPayloadSize`
  - `alaTestOamSaaConfigNumPkts`
  - `alaTestOamSaaConfigInterPktDelay`
  - `alaTestOamSaaConfigVlanPriority`
  - `alaTestOamSaaContinuous`

- `alaTestOamEtherConfigTable`
  - `alaTestOamIpv4ConfigTable`
show test-oam statistics

Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

**show test-oam** [string] statistics

---

### Syntax Definitions

**string** The name of an existing CPE test.

---

### Defaults

By default, statistics are displayed for all CPE tests.

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- Use the **string** parameter with this command to display statistics for a specific CPE test.
- The statistics displayed depend on the role the switch is performing for the test (generator or analyzer). For example, the analyzer switch may not show any packet count in the **TX** fields because it is the receiving switch.

---

### Examples

```
-> show test-oam Test1 statistics
Test-Id TX-Ingress TX-Egress RX-Ingress Remote-Stats Throughput (Mbps)
-----------------------------------------------
Test1 19017    19017    19017             19017        9.98

-> show test-oam statistics
Test-Id TX-Ingress TX-Egress RX-Ingress Remote-Stats Throughput (Mbps)
-----------------------------------------------
Test1 1200366 1200366 0      1200366          8
Test2 0        0       1200366 1200366          8
```

---

### output definitions

- **Test-Id** The CPE test name (ID).
- **TX-Ingress** The number of ingress test packets generated on the ingress UNI.
**output definitions**

<table>
<thead>
<tr>
<th>TX-Egress</th>
<th>The number of egress test packets transmitted on the egress NNI.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX-Ingress</td>
<td>The number of test packets received on the ingress NNI. This value is relevant on the receiving (analyzer) switch for the specific test.</td>
</tr>
<tr>
<td>Remote-Stats</td>
<td>The number of test frames received by the analyzer and fetched by the generator device.</td>
</tr>
<tr>
<td>Throughput (Mbps)</td>
<td>Displays the traffic throughput of the test.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **test-oam statistics flash-logging** Displays the CPE test configuration and status.
- **clear test-oam statistics** Clears CPE test statistics.

**MIB Objects**

- `alaTestOamStatsTable`
  - `alaTestOamConfigTestId`
  - `alaTestOamTxIngressCounter`
  - `alaTestOamTxEgressCounter`
  - `alaTestOamRxIngressCounter`
  - `alaTestOamRemoteStatsCounter`
  - `alaTestOamBandwidthThroughputStr`
**show test-oam saa statistics**

Displays the SAA test statistics for all CPE tests or for a specific test name.

```
show test-oam [string] saa statistics
```

**Syntax Definitions**

String

The name of an existing CPE test.

**Defaults**

By default, statistics are displayed for all CPE tests.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `string` parameter with this command to display SAA statistics for a specific CPE test.

**Examples**

```
-> show test-oam Test1 saa statistics
```

```
Test | Time of Last-Run | RTT Min RTT Avg RTT Max Jitter Min Jitter Avg Jitter Max Jitter Packets Sent Rcvd
-----|------------------|----------|---------|---------|--------|---------|--------|---------|--------|-----------|---------|----------|--------|---------|--------|---------|
Test1 2009-09-05 20:18:34.0 970 1067 1432 1 99 455 7 7 DEFAULT
```

```
-> show test-oam saa statistics
```

```
Test | Time of Last-Run | RTT Min RTT Avg RTT Max Jitter Min Jitter Avg Jitter Max Jitter Packets Sent Rcvd
-----|------------------|----------|---------|---------|--------|---------|--------|---------|--------|-----------|---------|----------|--------|---------|--------|---------|
Test1 2009-09-05 20:18:34.0 970 1067 1432 1 99 455 7 7 DEFAULT
Test2 2009-09-05 20:18:34.0 770 865 1432 2 99 255 7 7 DEFAULT
Test3 2009-09-05 40:38:34.0 770 967 1432 1 99 355 7 7 DEFAULT
Test4 2009-09-05 50:48:34.0 770 807 1432 1 99 255 7 7 DEFAULT
Test5 2009-09-06 60:18:34.0 640 867 1432 2 99 445 7 7 DEFAULT
Test6 2009-09-06 60:18:34.0 780 907 1432 3 99 255 7 7 DEFAULT
```

**output definitions**

<table>
<thead>
<tr>
<th>Test</th>
<th>The CPE test name (ID).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of Last-Run</td>
<td>Displays the date and time on which the test was last run.</td>
</tr>
<tr>
<td>RTT Min</td>
<td>Displays the minimum round trip time.</td>
</tr>
<tr>
<td>RTT Avg</td>
<td>Displays the average round trip time.</td>
</tr>
</tbody>
</table>
show test-oam saa statistics

output definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTT Max</td>
<td>Displays the maximum round trip time.</td>
</tr>
<tr>
<td>Jitter Min</td>
<td>Displays the minimum jitter value.</td>
</tr>
<tr>
<td>Jitter Avg</td>
<td>Displays the average jitter value.</td>
</tr>
<tr>
<td>Jitter Max</td>
<td>Displays the maximum jitter value.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Displays the number of packets sent during a single MAC ping.</td>
</tr>
<tr>
<td>Packets Recvd</td>
<td>Displays the number of packets received during a single MAC ping.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the Test Description parameter value for each test</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R1; command was introduced.

Related Commands

test-oam statistics flash-logging Displays the CPE test configuration and status.
clear test-oam statistics Clears CPE test statistics.

MIB Objects

alaTestOamSaaStatsTable
  alaTestOamConfigTestId
  alaTestOamSaaRunTime
  alaTestOamSaaPkttsSent
  alaTestOamSaaPkttsRcvd
  alaTestOamSaaMinRTT
  alaTestOamSaaAvgRTT
  alaTestOamSaaMaxRTT
  alaTestOamSaaMinJitter
  alaTestOamSaaAvgJitter
  alaTestOamSaaMaxJitter
clear test-oam statistics

Clears the statistics for all CPE tests or for a specific test name.

```
clear test-oam [string] statistics
```

**Syntax Definitions**

`string` The name of an existing CPE test.

**Defaults**

By default, statistics are cleared for all CPE tests.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `string` parameter with this command to clear the statistics for a specific CPE test.

**Examples**

```
-> clear test-oam Test1 statistics
-> clear test-oam statistics
```

**Release History**

Release 8.6R1; command was introduced.
Related Commands

**show test-oam statistics**  Displays the statistics for all CPE tests or for a specific test name. Use this command on both the generator and analyzer switch to determine test results.

**show test-oam saa statistics**  Displays the SAA test statistics for all CPE tests or for a specific test name.

MIB Objects

alaTestOamStatsTable
  alaTestOamConfigTestId
  alaTestOamStatsClearStats
test-oam group

Configures the CPE test group name and an optional description. The group name is used to identify and configure a CPE test group.

test-oam group string [descr description]

no test-oam group string

Syntax Definitions

string
The name of the CPE test group, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test-oam group.

description
The description to assign to the CPE test group, an alphanumeric string between 1 and 32 characters.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>DEFAULT</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900 C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to remove the specified CPE test group.
- This command creates a CPE test group that is identified by the test-oam name. Make sure the name specified does not exist in the switch configuration.
- To configure a CPE test group, the individual test must be configured.
- A maximum of 4 testoam profiles can be configured in a group to run the tests concurrently.
- Only one CPE test group can be active on the switch at any given time.
- Usage Guidelines for OmniSwitch 6560 and OmniSwitch 6570M:
  - A maximum of 8 testoam profiles can be configured in a group to run the tests concurrently.

Examples

-> test-oam group Testgroup1
-> test-oam group Testgroup2 descr second-testgroup
-> no test-oam group Testgroup1

Release History
Release 8.6R1; command was introduced.
Release 8.9R1; CPE test head group support added for OmniSwitch 6560.

Related Commands

**show test-oam group statistics** Displays the statistics for all CPE test groups or for a specific CPE test group. Use this command on both the generator and analyzer switch to determine test results.

**show test-oam group** Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects
alaTestOamGroupConfigTable
alaTestOamConfigGroupId
alaTestOamConfigGroupDescription
alaTestOamGroupConfigRowStatus
**test-oam group tests**

This defines the list of CPE test group tests that need to be added in the test-oam group.

```
test-oam group string [tests string1.......string8]
test-oam group string [no tests string1.......string8]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th><strong>string</strong></th>
<th>The name of the CPE test group, an alphanumeric string between 1 and 32 characters. This name is used to identify a specific CPE test group.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>string1.......string8</strong></td>
<td>The name of the configured test-oam tests.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command defines the list of test-oam tests that need to run concurrently.
- The test must exist, while configuring the test-oam list.
- A maximum of four tests can be configured to run concurrently.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of test-oam group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.
- Use the `no` form of the command to remove the test-oam tests from the CPE test group.
- Usage Guidelines for OmniSwitch 6560 and OmniSwitch 6570M:
  - A maximum of 8 tests can be configured to run concurrently.

### Examples

```
-> test-oam test1
-> test-oam test2
-> test-oam test3
```
-> test-oam test4
-> test-oam test5
-> test-oam test6
-> test-oam test7
-> test-oam test8
-> test-oam group Testgroup1 descr first-testgroup
-> test-oam group Testgroup1 tests test1 test2 test3 test4 test5 test6 test7 test8
-> test-oam group Testgroup1 no tests test1 test2 test3

**Release History**

Release 8.6R1; command was introduced.
Release 8.9R1; CPE test head group support added for OmniSwitch 6560.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show test-oam group</td>
<td>Displays the configuration and status of the CPE test groups.</td>
</tr>
<tr>
<td>show test-oam group</td>
<td>Displays the SAA statistics for all CPE test groups or for a specific CPE test group if mentioned.</td>
</tr>
</tbody>
</table>

**MIB Objects**

alaTestOamGroupFlowConfigTable
  alaTestOamConfigGroupId
  alaTestOamConfigTestId
  alaTestOamGroupFlowConfigRowStatus
test-oam feeder

This configures the feeder port globally in the system for CPE test group to feed the test traffic to generator port.

**test-oam feeder-port chassis/lot/port**

**no test-oam feeder-port**

### Syntax Definitions

**chassis/lot/port**

The port to be used to feed the test traffic only to generator port.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command configures the feeder port globally in the system.
- The feeder port cannot be the generator port and the generator port cannot be the feeder port.
- When a CPE test group is running, the modification to the feeder port shall not be allowed.
- Use the **no** form of the command to remove the feeder port from the system for CPE test group.

### Examples

```
-> test-oam feeder-port 1/1/4
-> no test-oam feeder-port
```

### Release History

Release 8.6R1; command was introduced.
Related Commands

- **test-oam group port**: Configures the port on which the CPE test group will run.
- **show test-oam group**: Displays the configuration and status of the CPE test groups.

MIB Objects

- `alaTestOamGlobalFeederPort`
test-oam group src-endpoint dst-endpoint

Configures the source and destination endpoints for the CPE test group.

```
<command>

Syntax Definitions

string | src_string | dst_string

string The name of an existing CPE test group.
src_string The management IP address or DNS host name of the switch that will transmit test traffic.
dst_string The management IP address or DNS host name of the switch that will receive test traffic. This is the switch on which traffic analysis is done.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>src-endpoint</td>
<td>DEFAULT</td>
</tr>
<tr>
<td>dst-endpoint</td>
<td>DEFAULT</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Using the DNS host name of the switch is highly recommended, as this name is unique and is mapped to an IP address configured for the switch.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of test-oam group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

```
-> test-oam group Testgroup1 src-endpoint SW1 dst-endpoint SW2
-> test-oam group Testgroup1 src-endpoint SW1
-> test-oam group Testgroup1 dst-endpoint SW2
```
**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- `test-oam group duration rate`  
  Configures the duration and rate for the specified CPE test group.

- `show test-oam group`  
  Displays the configuration and status of the CPE test groups.

**MIB Objects**

- `alaTestOamGroupConfigTable`
- `alaTestOamConfigGroupId`
- `alaTestOamGroupConfigSourceEndpoint`
- `alaTestOamGroupConfigDestinationEndpoint`
test-oam group role

Configures the role the switch will perform for the specified CPE test group. The type of role assigned determines whether the switch transmits (generator) or receives (analyzer) test frames.

test-oam group name role {generator | analyzer | loopback}

Syntax Definitions

name
   The name of an existing CPE test group.
generator
   Configures the switch as the test generator.
analyzer
   Configures the switch as the test analyzer.
loopback
   Configures the switch as loopback.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6900X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

Examples

-> test-oam group Testgroup1 role generator
-> test-oam group Testgroup2 role analyzer
-> test-oam group Testgroup2 role loopback

Release History

Release 8.6R1; command was introduced.
Related Commands

- **test-oam group duration rate**  Configures the duration and rate for the specified CPE test group.
- **show test-oam group**  Displays the configuration and status of the CPE test groups.

MIB Objects

- alaTestOamGroupConfigTable
  - alaTestOamConfigGroupId
  - alaTestOamGroupConfigRole
**test-oam group port**

Configures the port on which the CPE test group will run. Use this command on the switch that will generate the test traffic.

**Syntax Definitions**

```
string                  The name of an existing CPE test group.
chassis/slot/port       The port on which the CPE test will generate traffic.
```

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Configuring a port that is not in use is recommended. In addition, if the test port is a UNI port associated with an SAP profile, only that UNI port is used for the test. Traffic on other UNI ports associated with the same profile is *not* disrupted by the CPE test.
- This command automatically overwrites the port value previously configured for the specified CPE test group.
- The feeder port cannot be the generator port and the generator port cannot be the feeder port.
- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

**Examples**

```
-> test-oam group Testgroup1 port 1/1/2
```

**Release History**

Release 8.6R1; command was introduced.
Related Commands

**test-oam group start stop**  
Starts the traffic test for the CPE test group on the configured port or the given port.

**test-oam group remote-sys-mac**  
Stops the traffic test for the CPE test group on the configured port or the given port.

**show test-oam group**  
Displays the configuration and status of the CPE test groups.

MIB Objects

alaTestOamGroupConfigTable
  alaTestOamConfigGroupId
  alaTestOamGroupConfigPort
**test-oam group direction**

Configures the test direction of the test-oam group.

```
test-oam group string [direction {unidirectional | bidirectional}]
```

### Syntax Definitions

- `string` The name of an existing CPE test group.
- `direction` The direction of the CPE test group.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>direction</td>
<td>unidirectional</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

### Examples

- `-> test-oam group Testgroup1 direction unidirectional`
- `-> test-oam group Testgroup2 direction bidirectional`

### Release History

Release 8.6R1; command was introduced.
**Related Commands**

- **test-oam group duration rate**  Configures the duration and rate for the specified CPE test group.
- **show test-oam group**  Displays the configuration and status of the CPE test groups.

**MIB Objects**

- `alaTestOamGroupConfigTable`
  - `alaTestOamConfigGroupId`
  - `alaTestOamGroupConfigDirection`
**test-oam group duration rate**

Configures the duration and rate for the specified test-oam group. Use this command to configure these test parameters on the generator switch.

**Syntax**

```
(test-oam group string [duration secs] [rate rate])
```

**Syntax Definitions**

- **string**
  - The name of an existing CPE test group.

- **secs**
  - The duration of the test, in seconds. This is the amount of time the generator will actively transmit test packets to the remote (analyzer) switch. The valid time range is 5–3600 seconds.

- **rate**
  - The rate, in Kbps or Mbps, at which test traffic is generated. The minimum value allowed is 8 Kbps to line rate. The granularity of the transmit rate is 8 Kbps for 100 Mbps port and 2 Mbps for 1Gig ports.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>secs</td>
<td>5 secs</td>
</tr>
<tr>
<td>rate</td>
<td>8 k</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command automatically overwrites any duration and rate parameter values previously configured for the specified CPE test group.

- The status of the CPE test group will change to “ended” when the test duration time expires.

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.

- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.

- When a CPE test group is running, the modification of a feeder port shall not be allowed.

**Examples**

```
-> test-oam group Testgroup1 duration 10
```
CPE Test Head Commands

test-oam group duration rate

-> test-oam group Testgroup1 rate 8m
-> test-oam group Testgroup1 duration 10 rate 8m

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group Displays the configuration and status of the CPE test groups.

MIB Objects

alaTestOamGroupConfigTable
  alaTestOamConfigGroupId
  alaTestOamGroupConfigDuration
  alaTestOamGroupConfigGeneratorBandwidth
test-oam group start stop

Starts or stops the traffic test for the test-oam group on the configured port or the given port.

test-oam group string \{\{port chassis/slot/port\} start | stop\} [fetch-remote-stats]

Syntax Definitions

string The name of an existing CPE test group.
chassis/slot/port The port on which the CPE test group will generate traffic.
start Enables the test.
stop Disables the test.
fetch-remote-stats Triggers the group test at the remote device from the generator. The statistics are collected during the test and the test is stopped after receiving the test results.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

• When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.

• When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.

• When a CPE test group is running, the modification of a feeder port shall not be allowed.

• Use the fetch-remote-stats parameter to collect the test statistics from the remote device.

Examples

- test-oam group Testgroup1 port 1/1/2 start
- test-oam group Testgroup2 start
- test-oam group Testgroup1 start fetch-remote-stats
- test-oam group testgroup2 port 1/1/2 start fetch-remote-stats
- test-oam group Testgroup1 stop
- test-oam group Testgroup2 stop
**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- `show test-oam group` Displays the configuration and status of the CPE test groups.

**MIB Objects**

- `alaTestOamGroupConfigTable`  
  - `alaTestOamConfigGroupId`  
  - `alaTestOamGroupConfigPort`  
  - `alaTestOamGroupConfigState`  
  - `alaTestOamGroupConfigRemoteStatsFetchState`
test-oam group remote-sys-mac

Configures the system MAC address of the remote device to receive test OAM messages.

```
test-oam group string remote-sys-mac string
```

**Syntax Definitions**

- **string**: The name of an existing CPE test group.
- **remote-sys-mac**: The system MAC address of the remote device.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command on the switch to set the system MAC address of the remote device to receive the test OAM messages.
- The remote-sys-mac must be the primary CMM MAC address of the remote device.
- The remote-sys-mac is not applicable for analyzer or loopback.

**Examples**

```
-> test-oam group Testgroup1 remote-sys-mac 00:e0:b1:7c:7a:fa
```

**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- `show test-oam group` Displays the configuration and status of the CPE test groups.

**MIB Objects**

- `alaTestOamGroupConfigTable`
- `alaTestOamGroupConfigRemoteSysMacAddress`
clear test-oam group statistics

This clears the statistics of the CPE test group.

clear test-oam group string statistics

**Syntax Definitions**

string

The name of an existing CPE test group.

statistics

Clears the statistics for the give CPE test group.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When a CPE test group is running, the modification of a test which is part of the group shall not be allowed.
- When a CPE test group is running, the modification of CPE test group parameters shall not be allowed.
- When a CPE test group is running, the modification of a feeder port shall not be allowed.

**Examples**

-> clear test-oam group Testgroup1 statistics (Clears the statistics for the specified test-oam group)

-> clear test-oam group statistics (Clears the statistics for all the test-oam groups)

**Release History**

Release 8.6R1; command was introduced.
Related Commands

**show test-oam group statistics**  Displays the statistics for all test-oam groups or for a specific CPE test group.

**show test-oam group**  Displays the configuration and status of the CPE test groups.

MIB Objects

alaTestOamGroupConfigTable
  alaTestOamConfigGroupId
  alaTestOamGroupConfigStatsClear
  alaTestOamGlobalGroupClearStats
**show test-oam group**

Displays the configuration and status of the CPE test groups.

`show test-oam group [tests | string]`

---

**Syntax Definitions**

- **tests**
  - Displays information for all the CPE test groups.

- **string**
  - The name of an existing CPE test group.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **tests** parameter to display information for all CPE test groups configured on the switch.

- Use the **string** parameter to display detailed information for a specific CPE test group.

---

**Examples**

```plaintext
-> show test-oam group tests
Total Test-Groups: 2
Feeder Port : none
Test-Group Port Duration Rate Nb of Flows Direction Status Remote-Sys-Mac
----------+-----+----------+---------+-----+---------------+------------+---------------------
Testgroup1 none 5          -     2 unidirectional not-started 00:00:00:00:00:00:00
Testgroup2 none 5          -     3 unidirectional not-started 00:00:00:00:00:00:00
```

---

**output definitions**

- **Test-Groups**
  - The CPE test group. Configured through the `test-oam group` command.

- **Port**
  - The port on which the test is run.

- **Duration**
  - The amount of time the test will run.

- **Rate**
  - The rate at which packets are transmitted on the test port. Configured through the `test-oam group duration rate` command.

- **Nb of Flows**
  - Number of test flows configured for the respective CPE test group.
output definitions

<table>
<thead>
<tr>
<th>Direction</th>
<th>The direction of the test traffic. Note that only unidirectional traffic tests are supported.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The operational status of the test.</td>
</tr>
<tr>
<td>Remote-Sys-Mac</td>
<td>The MAC address of the remote device configured through the <code>test-oam group remote-sys-mac</code> command.</td>
</tr>
</tbody>
</table>

`-> show test-oam group Testgroup1
Legend: Port: * = Inactive port`

TEST Parameters for Testgroup1:
- **Source Endpoint**: SW1
- **Destination Endpoint**: SW2
- **Test Group Description**: first-testgroup
- **Direction**: bidirectional
- **Role**: generator
- **Tx Rate**: 10m
- **Duration**: 60 (secs)
- **Port**: 1/5
- **State**: stop
- **Status**: not-started

**Flow 1:**
- **Test Name**: test1
- **Vlan**: 1001
- **Tx Rate**: 10m
- **Source MAC**: 00:11:22:12:44:55
- **Destination MAC**: 00:22:33:12:55:66
- **Frame Size**: 64
- **L2-SAA DE**: False
- **L2-SAA Payload Size**: 64
- **L2-SAA Count**: 5
- **L2-SAA Interval**: 1000
- **L2-SAA Priority**: 0
- **L2-SAA Continuous**: no

**Flow 2:**
- **Test Name**: test2
- **Vlan**: 1001
- **Tx Rate**: 10m
- **Source MAC**: 00:11:22:13:44:55
- **Frame Size**: 100
- **L2-SAA DE**: True
- **L2-SAA Payload Size**: 120
- **L2-SAA Count**: 0
- **L2-SAA Interval**: 900
- **L2-SAA Priority**: 6
- **L2-SAA Continuous**: yes

**Flow 3:**
- **Test Name**: test3
- **Vlan**: 1001
- **Tx Rate**: 10m
- **Source MAC**: 00:11:22:14:44:55
- **Destination MAC**: 00:22:33:14:55:66
Frame Size : 100,
L2-SAA DE : True,
L2-SAA Payload Size : 120,
L2-SAA Count : 0,
L2-SAA Interval : 900,
L2-SAA Priority : 6
L2-SAA Continuous : yes

Flow 4:
Test Name : test4,
Vlan : 1001,
Tx Rate : 10m,
Source MAC : 00:11:22:15:44:55,
Destination MAC : 00:22:33:15:55:66,
Remote Sys MAC : E8:E7:32:32:A6:EE,
Frame Size : 100
L2-SAA DE : True,
L2-SAA Payload Size : 120,
L2-SAA Count : 0,
L2-SAA Interval : 900,
L2-SAA Priority : 6
L2-SAA Continuous : yes

output definitions

<table>
<thead>
<tr>
<th>Test-Groups</th>
<th>The CPE test group. Configured through the <code>test-oam group</code> command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port on which the test is run.</td>
</tr>
<tr>
<td>Source Endpoint</td>
<td>The host name for the source (generator) switch. Configured through the <code>test-oam group src-endpoint dst-endpoint</code> command.</td>
</tr>
<tr>
<td>Destination Endpoint</td>
<td>The host name for the destination (analyzer) switch. Configured through the <code>test-oam group src-endpoint dst-endpoint</code> command.</td>
</tr>
<tr>
<td>Source Mac</td>
<td>The source MAC address of the test frame. Configured through the <code>test-oam vlan test-frame</code> command.</td>
</tr>
<tr>
<td>Destination Mac</td>
<td>The destination MAC address of the test frame. Configured through the <code>test-oam vlan test-frame</code> command.</td>
</tr>
<tr>
<td>Remote Sys Mac</td>
<td>The MAC address of the remote device configured through the <code>test-oam group remote-sys-mac</code> command.</td>
</tr>
<tr>
<td>Duration</td>
<td>The amount of time the test will run.</td>
</tr>
<tr>
<td>Role</td>
<td>The role of the switch for this test (generator or analyzer). Configured through the <code>test-oam role</code> command.</td>
</tr>
<tr>
<td>Rate</td>
<td>The rate at which packets are transmitted on the test port. Configured through the <code>test-oam group duration rate</code> command.</td>
</tr>
<tr>
<td>Frame Size</td>
<td>The size of the test frame. Configured through the <code>test-oam group duration rate</code> command.</td>
</tr>
<tr>
<td>Direction</td>
<td>The direction of the test traffic. Note that only unidirectional traffic tests are supported.</td>
</tr>
<tr>
<td>Status</td>
<td>The operational status of the test.</td>
</tr>
<tr>
<td>L2-SAA Count</td>
<td>Specifies the number of packets sent in one MAC ping iteration.</td>
</tr>
<tr>
<td>L2-SAA Interval</td>
<td>Specifies the delay between two consecutive packets transmitted during a MAC ping iteration.</td>
</tr>
</tbody>
</table>
show test-oam group

output definitions

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>L2-SAA DE</td>
<td>Specifies if the drop enable bit value is used.</td>
</tr>
<tr>
<td>L2-SAA Payload Size</td>
<td>Specifies the size of the MAC ping payload used for the MAC ping operation.</td>
</tr>
<tr>
<td>L2-SAA Priority</td>
<td>Specifies the priority value set for the L2 SAA frames.</td>
</tr>
<tr>
<td>L2-SAA Continuous</td>
<td>Specifies the SAA session will run continuously until the test-oam session ends.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R1; command was introduced.

Related Commands

show test-oam group Displays the statistics for all CPE test groups or for a specific CPE test group.

MIB Objects

alaTestOamGlobalFeederPort
alaTestOamGroupConfigTable
alaTestOamGroupConfigRowStatus
  alaTestOamConfigGroupId
  alaTestOamGroupConfigPort
  alaTestOamGroupConfigDuration
  alaTestOamGroupConfigGeneratorBandwidth
  alaTestOamGroupConfigFlowCount
  alaTestOamGroupConfigDirection
  alaTestOamGroupConfigStatus
  alaTestOamGroupConfigRemoteStatsFetchState
  alaTestOamGroupConfigRemoteSysMacAddress
alaTestOamGroupConfigTable
  alaTestOamConfigGroupId
  alaTestOamGroupConfigSourceEndpoint
  alaTestOamGroupConfigDestinationEndpoint
  alaTestOamConfigGroupDescription
  alaTestOamGroupConfigDirection
  alaTestOamGroupConfigRole
  alaTestOamGroupConfigGeneratorBandwidth
  alaTestOamGroupConfigDuration
  alaTestOamGroupConfigPort
  alaTestOamGroupConfigState
  alaTestOamGroupConfigStatus
  alaTestOamGroupConfigStatsClear
alaTestOamGroupFlowConfigTable
  alaTestOamConfigTestId
  alaTestOamGroupFlowVlan
  alaTestOamConfigGroupId
  alaTestOamGroupFlowGeneratorBandwidth
  alaTestOamGroupFlowFrameSrcMacAddress
  alaTestOamGroupFlowFrameDstMacAddress
  alaTestOamGroupFlowGeneratorPacketSize
show test-oam group saa statistics

Displays the SAA test statistics for all CPE test groups or for a specific test name.

show test-oam group [string] saa statistics

Syntax Definitions

string

The name of an existing CPE test group.

Defaults

By default, statistics are displayed for all CPE test group.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the string parameter with this command to display SAA statistics for a specific CPE test group.

Examples

-> show test-oam group Test1 saa statistics

<table>
<thead>
<tr>
<th>Test-group Flow Time of Last-Run</th>
<th>RTT Min</th>
<th>RTT Avg</th>
<th>RTT Max</th>
<th>Jitter Jitter Jitter</th>
<th>Packets Sent</th>
<th>Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test1</td>
<td>2009-09-05,20:18:34.0</td>
<td>970</td>
<td>1067</td>
<td>1432</td>
<td>1</td>
<td>99</td>
</tr>
</tbody>
</table>

-> show test-oam group saa statistics

<table>
<thead>
<tr>
<th>Test-group Flow Time of Last-Run</th>
<th>RTT Min</th>
<th>RTT Avg</th>
<th>RTT Max</th>
<th>Jitter Jitter Jitter</th>
<th>Packets Sent</th>
<th>Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latest Record:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test1</td>
<td>2009-09-05,20:18:34.0</td>
<td>970</td>
<td>1067</td>
<td>1432</td>
<td>1</td>
<td>99</td>
</tr>
<tr>
<td>Test2</td>
<td>2009-09-05,30:28:34.0</td>
<td>770</td>
<td>865</td>
<td>1432</td>
<td>2</td>
<td>99</td>
</tr>
<tr>
<td>Test3</td>
<td>2009-09-05,40:38:34.0</td>
<td>570</td>
<td>967</td>
<td>1432</td>
<td>3</td>
<td>99</td>
</tr>
<tr>
<td>Test4</td>
<td>2009-09-05,50:48:34.0</td>
<td>770</td>
<td>807</td>
<td>1432</td>
<td>1</td>
<td>99</td>
</tr>
<tr>
<td>Test5</td>
<td>2009-09-06,20:18:34.0</td>
<td>640</td>
<td>867</td>
<td>1432</td>
<td>2</td>
<td>99</td>
</tr>
<tr>
<td>Test6</td>
<td>2009-09-06,30:18:34.0</td>
<td>780</td>
<td>907</td>
<td>1432</td>
<td>3</td>
<td>99</td>
</tr>
</tbody>
</table>

output definitions

Test-group

The CPE test group name (ID).

Flow

Displays the flow identifier for the test.

Time of Last-Run

Displays the date and time on which the test was last run.
show test-oam group saa statistics

**output definitions**

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>RTT Min</td>
<td>Displays the minimum round trip time.</td>
</tr>
<tr>
<td>RTT Avg</td>
<td>Displays the average round trip time.</td>
</tr>
<tr>
<td>RTT Max</td>
<td>Displays the maximum round trip time.</td>
</tr>
<tr>
<td>Jitter Min</td>
<td>Displays the minimum jitter value.</td>
</tr>
<tr>
<td>Jitter Avg</td>
<td>Displays the average jitter value.</td>
</tr>
<tr>
<td>Jitter Max</td>
<td>Displays the maximum jitter value.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Displays the number of packets sent during a single MAC ping.</td>
</tr>
<tr>
<td>Packets Rcvd</td>
<td>Displays the number of packets received during a single MAC ping.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description for each provided by the user during the test creation. By default it is displayed as &quot;DEFAULT&quot;.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **show test-oam group**
  Displays the configuration and status of the CPE test groups.
- **clear test-oam group statistics**
  This clears the statistics of the CPE test group.

**MIB Objects**

alaTestOamGroupFlowSaaStats

- alaTestOamConfigGroupId
- alaTestOamConfigTestId
- alaTestOamGroupFlowSaaStatsEntry
- alaTestOamGroupFlowSaaRunTime
- alaTestOamGroupFlowSaaPktsSent
- alaTestOamGroupFlowSaaPktsRcvd
- alaTestOamGroupFlowSaaRunTime
- alaTestOamGroupFlowSaaMinRTT
- alaTestOamGroupFlowSaaAvgRTT
- alaTestOamGroupFlowSaaMaxRTT
- alaTestOamGroupFlowSaaMinJitter
- alaTestOamGroupFlowSaaAvgJitter
- alaTestOamGroupFlowSaaMaxJitter
### show test-oam group statistics

Displays the statistics for all CPE test groups or for a specific CPE test group. Use this command on both the generator and analyzer switch to determine test results.

**show test-oam group [string] statistics**

---

**Syntax Definitions**

*string* 

The name of an existing CPE test group.

**Defaults**

By default, statistics are displayed for all CPE test groups.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the *string* parameter with this command to display statistics for a specific CPE test group.
- The statistics displayed depend on the role the switch is performing for the test (generator or analyzer). For example, the analyzer switch may not show any packet count in the **TX** fields because it is the receiving switch.

**Examples**

```bash
-> show test-oam group TestGroup4 statistics
Test-Group Flow TX-Ingress TX-Egress RX-Ingress Remote-Stats Throughput(Mbps)
-----------------------------------------------+----------------+---------------+------------+-------------+----------------+
TestGroup4 flow1 19017 19017 0 19017
TestGroup4 flow2 19017 19017 0 19017

-> show test-oam group statistics
Test-Group Flow TX-Ingress TX-Egress RX-Ingress Remote-Stats Throughput(Mbps)
-----------------------------------------------+----------------+---------------+------------+-------------+----------------+
Testgroup1 test1 20163463 17205475 0 17205475 172.05
Testgroup1 test2 20720137 17680541 0 17680541 176.81
Testgroup1 test3 20709603 17668483 0 17668483 176.68
Testgroup1 test4 20698156 17656987 0 17656987 176.57
Testgroup2 test1 20163463 17205475 0 17205475 172.05
Testgroup2 test2 20720137 17680541 0 17680541 176.81
Testgroup2 test3 20709603 17668483 0 17668483 176.68
Testgroup2 test4 20698156 17656987 0 17656987 176.57
```
**Output Definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test-Group</td>
<td>The CPE test group.</td>
</tr>
<tr>
<td>TX-Ingress</td>
<td>The number of ingress test packets generated on the ingress UNI.</td>
</tr>
<tr>
<td>TX-Egress</td>
<td>The number of egress test packets transmitted on the egress NNI.</td>
</tr>
<tr>
<td>RX-Ingress</td>
<td>The number of test packets received on the ingress NNI. This value is</td>
</tr>
<tr>
<td></td>
<td>relevant on the receiving (analyzer) switch for the specific test.</td>
</tr>
<tr>
<td>Remote-Stats</td>
<td>The number of test frames received by the analyzer and fetched by the</td>
</tr>
<tr>
<td></td>
<td>generator device.</td>
</tr>
<tr>
<td>Throughput(Mbps)</td>
<td>Displays the traffic throughput of the test.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- `show test-oam group` Displays the configuration and status of the CPE test groups.
- `test-oam group remote-sys-mac` Clears the statistics of the CPE test group.

**MIB Objects**

- `alaTestOamGroupFlowStatsTable`
  - `alaTestOamConfigGroupId`
  - `alaTestOamConfigTestId`
  - `alaTestOamGroupFlowTxIngressCounter`
  - `alaTestOamGroupFlowTxEgressCounter`
  - `alaTestOamGroupFlowRxIngressCounter`
  - `alaTestOamGroupFlowRemoteStatsCounter`
  - `alaTestOamGroupBandwidthThroughputStr`
56  PPPoE Intermediate Agent

Point-to-Point Protocol over Ethernet (PPPoE) provides the ability to connect a network of hosts to a Remote Access Concentrator. For example, Broadband Network Gateway over a simple bridging access device. In PPPoE model, each host utilizes its own Point-to-Point Protocol (PPP) stack and the user is presented with a familiar user interface. By using PPPoE, Access control, billing, and type of service can be configured on a per-user, rather than a per-site, basis.

PPPoE Intermediate Agent (PPPoE-IA) solution is designed for the PPPoE access method and is based on the Access Node implementing a PPPoE-IA function to insert access loop identification in PPPoE discovery packets (PADI/PADR/PADT) received from the user side.

MIB information for the PPPoE-IA commands is as follows:

   *Filename*: alcatel-ind1-pppoe-ia-mib.mib
   *Module*: ALCATEL-IND1-PPPOEIA-MIB

A summary of the available commands is listed here.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>pppoe-ia</td>
</tr>
<tr>
<td>pppoe-ia {port</td>
</tr>
<tr>
<td>pppoe-ia {trust</td>
</tr>
<tr>
<td>pppoe-ia access-node-id</td>
</tr>
<tr>
<td>pppoe-ia circuit-id</td>
</tr>
<tr>
<td>pppoe-ia remote-id</td>
</tr>
<tr>
<td>clear pppoe-ia statistics</td>
</tr>
<tr>
<td>show pppoe-ia configuration</td>
</tr>
<tr>
<td>show pppoe-ia {port</td>
</tr>
<tr>
<td>show pppoe-ia statistics</td>
</tr>
</tbody>
</table>

Configuration procedures for PPPoE-IA are explained in the “Configuring PPPoE Intermediate Agent” chapter of the *OmniSwitch AOS Release 8 Network Configuration Guide*. 
pppoe-ia

Enable or disable PPPoE-IA globally on the switch.

pppoe-ia {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enable PPPoE-IA.</td>
</tr>
<tr>
<td>disable</td>
<td>Disable PPPoE-IA.</td>
</tr>
</tbody>
</table>

Defaults

By default, PPPoE-IA is disabled globally on the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

All PPPoE-IA parameters are configurable irrespective of the global status of PPPoE-IA.

Examples

-> pppoe-ia enable
-> pppoe-ia disable

Release History

Release 8.6R1; command introduced.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`pppoe-ia {port</td>
<td>linkagg}`</td>
</tr>
<tr>
<td>`pppoe-ia {trust</td>
<td>client}`</td>
</tr>
<tr>
<td><code>pppoe-ia access-node-id</code></td>
<td>Globally configures a format to form an identifier that uniquely identifies an access node.</td>
</tr>
<tr>
<td><code>pppoe-ia circuit-id</code></td>
<td>Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.</td>
</tr>
<tr>
<td><code>pppoe-ia remote-id</code></td>
<td>Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.</td>
</tr>
<tr>
<td><code>clear pppoe-ia statistics</code></td>
<td>Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.</td>
</tr>
<tr>
<td><code>show pppoe-ia configuration</code></td>
<td>Displays the global configuration for PPPoE-IA.</td>
</tr>
<tr>
<td>`show pppoe-ia {port</td>
<td>linkagg}`</td>
</tr>
<tr>
<td><code>show pppoe-ia statistics</code></td>
<td>Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.</td>
</tr>
</tbody>
</table>

### MIB Objects

- alaPPPoEIAGlobalStatus
**pppoe-ia {port | linkagg}**

Enable or disable PPPoE-IA on a port or a link aggregate port. Link aggregate can be either static or dynamic.

**pppoe-ia {port chassis/slot/port[-port2] | linkagg agg_num} {enable | disable}**

### Syntax Definitions

- **chassis**
  - The chassis identifier.

- **slot**
  - The slot number for the module.

- **port**
  - Port number of the interface to be configured.

- **port2**
  - Last port number in a range of ports to be configured.

- **linkagg agg_num**
  - The link aggregate identification number.

- **enable**
  - Enable PPPoE-IA on a port.

- **disable**
  - Disable PPPoE-IA on a port.

### Defaults

By default, PPPoE-IA is disabled on all ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- All PPPoE-IA parameters are configurable irrespective of the per-port PPPoE-IA status (enabled or disabled).

- PPPoE-IA must be enabled globally as well as on a port.

- PPPoE-IA is not supported on port mirroring destination ports. However, the configurations are accepted.

- PPPoE-IA is not supported on aggregable ports.

### Examples

- -> pppoe-ia port 1/1/1 enable
- -> pppoe-ia port 1/1/4 disable
- -> pppoe-ia linkagg 1 enable
Release History

Release 8.6R1; command introduced.

Related Commands

- **pppoe-ia**
  Enable or disable PPPoE-IA globally on the switch.

- **show pppoe-ia configuration**
  Displays the global configuration for PPPoE-IA.

- **show pppoe-ia {port | linkagg}**
  Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.

- **show pppoe-ia statistics**
  Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

- **alaPPPoEIAPortConfigTable**
- **alaPPPoEIAPortConfigStatus**
**pppoe-ia {trust | client}**

Configures a port or a link aggregate port as trusted or client port for PPPoE-IA.

A trust port is a port that is connected to the Broadband Network Gateway whereas a client port is connected to the host.

```
pppoe-ia {port chassis/slot/port[-port2] | linkagg agg_num} {trust | client}
```

### Syntax Definitions

- **chassis**
  - The chassis identifier.
- **slot**
  - The slot number for the module.
- **port**
  - Port number of the interface to be configured.
- **port2**
  - Last port number in a range of ports to be configured.
- **linkagg agg_num**
  - Specifies the link aggregate identification number.
- **trust**
  - Specifies the mode of the port as trust.
- **client**
  - Specifies the mode of the port as client.

### Defaults

By default, all ports are client ports.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- All PPPoE-IA parameters are configurable irrespective of per-port PPPoE-IA status (enabled or disabled).
- PPPoE-IA must be enabled globally as well as on a port.
- For PPPoE-IA to work, it must be enabled on a client port as well as a trusted port.
- PPPoE-IA is not supported on aggregable ports.
- PPPoE-IA is not supported on port mirroring destination ports; however, the configurations are accepted.

### Examples

```
-> pppoe-ia port 1/1 /1
```
PPPoE Intermediate Agent

ppoe-ia {trust | client}

-> pppoe-ia port 1/1/2-4 client
-> pppoe-ia linkagg 7 trust
-> pppoe-ia linkagg 0 client

Release History
Release 8.6R1; command introduced.

Related Commands

ppoe-ia
Enable or disable PPPoE-IA globally on the switch.

ppoe-ia {port | linkagg}
Enable or disable PPPoE-IA on a port or a link aggregate port.

ppoe-ia {trust | client}
Configures a port or a link aggregate port as trust or client port for PPPoE-IA.

show pppoe-ia configuration
Displays the global configuration for PPPoE-IA.

show pppoe-ia {port | linkagg}
Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.

show pppoe-ia statistics
Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects
alaPPPoEIAPortConfigTable
alaPPPoEIAPortConfigTrustMode
**pppoe-ia access-node-id**

Globally configures a format to form an identifier that uniquely identifies an access node.

```plaintext
pppoe-ia access-node-id {base-mac | system-name | mgnt-address | user-string string}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>base-mac</td>
<td>The base MAC address of the switch.</td>
</tr>
<tr>
<td>system-name</td>
<td>The configured name of the switch.</td>
</tr>
<tr>
<td>mgnt-address</td>
<td>The IP address of the management interface of the switch.</td>
</tr>
<tr>
<td>string</td>
<td>The value of user configured string.</td>
</tr>
</tbody>
</table>

### Defaults

By default, PPPoE-IA uses the base MAC address of the switch as the Access-Node-Identifier.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/</td>
<td>No</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>No</td>
</tr>
<tr>
<td>9900 X48C2/T24C2/</td>
<td>Yes</td>
</tr>
<tr>
<td>9900 X24C2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The access-node-identifier can have a maximum of 32 characters. The access-node-identifier longer than 32 characters is truncated to 32 characters.
- The access-node-identifier when configured as user-string must not contain spaces.
- The value of user string must not be NULL.
- In case of management address format, IP address of the Loopback0 interface (if configured and active) or the first active IP interface address is used as the management address. If none of them are available, IP address ‘0.0.0.0’ is used as management address.
- If the access-node-identifier is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.

### Examples

```plaintext
-> pppoe-ia access-node-id base-mac
-> pppoe-ia access-node-id user-string accessnode1
```
**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- `pppoe-ia`  
  Enable or disable PPPoE-IA globally on the switch.

- `pppoe-ia {port | linkagg}`  
  Enables or disables PPPoE-IA on a port or a link aggregate port.

- `pppoe-ia {trust | client}`  
  Configures a port or a link aggregate port as trust or client port for PPPoE-IA.

- `clear pppoe-ia statistics`  
  Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.

- `show pppoe-ia configuration`  
  Displays the global configuration for PPPoE-IA.

- `show pppoe-ia {port | linkagg}`  
  Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.

- `show pppoe-ia statistics`  
  Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

**MIB Objects**

- `alaPPPoEIAGlobalAccessNodeIDFormatType`
- `alaPPPoEIAGlobalAccessNodeIDStringValue`
**pppoe-ia circuit-id**

Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop that receives the PPPoE Active Discovery Initiation (PADI) or PPPoE Active Discovery Request (PADR) or PPPoE Active Discovery Terminate (PADT) from the user end.

`pppoe-ia circuit-id {default [atm] ascii [base-mac | system-name | interface | vlan | cvlan | interface-alias | user-string string | delimiter char}]`

**Syntax Definitions**

- **default**
  The default value of the Circuit-ID used for the Ethernet parameter.

- **atm**
  When the PPPoE-IA Circuit-ID format is configured as “default atm” the Circuit-ID encoding happens for “ATM” (Asynchronous Transfer Mode) parameter.

- **ascii**
  Circuit-ID format used to configure Circuit-ID string using the five parameters and delimiter. Maximum five parameters can be selected from the given seven options: base-mac, system-name, interface, vlan, cvlan, interface-alias, and user-string.

- **base-mac**
  The base MAC address of the switch.

- **system-name**
  Name configured for the switch.

- **interface**
  The interface on which the PPPoE message is received.

- **vlan**
  VLAN interface on which the PPPoE message is received.

- **cvlan**
  Inner-VLAN or customer VLAN of the PPPoE message.

- **interface-alias**
  Configured alias of the interface on which the PPPoE message is received.

- **string**
  The value of user configured string.

- **delimiter**
  A user configurable delimiter used to separate the fields of an ASCII string forming the Circuit-ID.

- **char**
  The value (a character) of the user configurable delimiter.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>char</td>
<td>:</td>
</tr>
</tbody>
</table>

By default, “:” (colon) is used as the delimiter.
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platforms Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
</tr>
<tr>
<td>6465</td>
</tr>
<tr>
<td>6560</td>
</tr>
<tr>
<td>6570M</td>
</tr>
<tr>
<td>6860</td>
</tr>
<tr>
<td>6860N</td>
</tr>
<tr>
<td>6865</td>
</tr>
<tr>
<td>6900</td>
</tr>
<tr>
<td>6900 V72/C32</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
</tr>
<tr>
<td>6900 X48C6/V48C8</td>
</tr>
<tr>
<td>9900 C32E/T24C2</td>
</tr>
<tr>
<td>9900 X24C2</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Circuit-ID identification is configurable only globally and cannot be configured on a per-port or per-VLAN basis.
- To configure ethernet default parameter, use “default” in the CLI command.
- To configure default parameter as “atm”, use “default ATM” in the CLI command.
- When the PPPoE-IA Circuit-ID format is configured as “default atm” the Circuit-ID encoding happens for “ATM” (Asynchronous Transfer Mode) parameter.
- By default, the value of the Circuit-ID is "access-node-id eth slot/port[:vlan-id]". For example, if the value of access-node-id is "vxTarget", the default value of Circuit-ID is "vxTarget eth 1/1:10", if the packet is received on the interface 1/1 in vlan 10.
- By default, the delimiter used is “:”. The available delimiters are: “:” (colon), “|” (pipe), “/” (forward slash), “\” (backward slash), “_” (hyphen), “_” (underscore), “ “ (space), “#” (hash), “.” (full stop), “,” (comma), “;” (semicolon).
- The Circuit-ID can have a maximum of 63 characters. The Circuit-ID longer than 63 characters is truncated to 63 characters.
- At most, five fields out of the available seven is encoded for the Circuit-ID in the order specified by the user.
- If the access-node-identifier is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.
- The value of user string must not be NULL.
- You can configure the same Circuit-ID format multiple times (for example, base MAC address of the switch can be configured multiple times in ASCII format of Circuit-ID).
- If the Circuit-ID format is default, irrespective of the ASCII fields (if configured), the Circuit-ID configuration is not visible in `show pppoe-ia configuration` output.

Examples

```
-> pppoe-ia circuit-id default
-> pppoe-ia circuit-id default atm
-> pppoe-ia circuit-id ascii base-mac vlan
-> pppoe-ia circuit-id ascii system-name interface user-string cid1
-> pppoe-ia circuit-id ascii system-name delimiter #
```
Release History

Release 8.6R1; command introduced.

Related Commands

- **pppoe-ia**: Enable or disable PPPoE-IA globally on the switch.
- **pppoe-ia {trust | client}**: Configures a port or a link aggregate port as trust or client port for PPPoE-IA.
- **show pppoe-ia configuration**: Displays the global configuration for PPPoE-IA.
- **show pppoe-ia {port | linkagg}**: Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.
- **show pppoe-ia statistics**: Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

MIB Objects

- alaPPPoEIAGlobalCircuitIDFormatType
- alaPPPoEIAGlobalCircuitIDField1
- alaPPPoEIAGlobalCircuitIDField1StrVal
- alaPPPoEIAGlobalCircuitIDField2
- alaPPPoEIAGlobalCircuitIDField2StrVal
- alaPPPoEIAGlobalCircuitIDField3
- alaPPPoEIAGlobalCircuitIDField3StrVal
- alaPPPoEIAGlobalCircuitIDField4
- alaPPPoEIAGlobalCircuitIDField4StrVal
- alaPPPoEIAGlobalCircuitIDField5
- alaPPPoEIAGlobalCircuitIDField5StrVal
- alaPPPoEIAGlobalCircuitIDDelimiter
**pppoe-ia remote-id**

Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.

`pppoe-ia remote-id {base-mac | system-name | mgnt-address | user-string string}`

**Syntax Definitions**

- **base-mac**: The base MAC address of the switch.
- **system-name**: The name configured for the switch.
- **mgnt-address**: The management IP address of the switch.
- **string**: The value configured for user string.

**Defaults**

By default, the base MAC address of the switch is used as the format for Remote-ID.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Remote-ID is configurable only globally and cannot be configured on a per-port or per-VLAN basis.
- Remote-ID can have a maximum of 63 characters. The Remote-ID longer than 63 characters is truncated to 63 characters.
- In case of management address format, IP address of the Loopback0 interface (if configured and active) or the first active IP interface address is used as the management address. If none of them are available, IP address ‘0.0.0.0’ is used as management address.
- If the Remote-ID is configured as any other format other than user-string format, then the string value configuration is not allowed through SNMP or Web View application.
- It is mandatory to provide the string value through SNMP using Multi-varbind for the user-string format.
- The value of user string must not be NULL.

**Examples**

- `pppoe-ia remote-id base-mac`
- `pppoe-ia remote-id user-string remoteuser1`
**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- **pppoe-ia**
  
  Enable or disable PPPoE-IA globally on the switch.

- **pppoe-ia {trust | client}**
  
  Configures a port or a link aggregate port as trust or client port for PPPoE-IA.

- **show pppoe-ia configuration**
  
  Displays the global configuration for PPPoE-IA.

- **show pppoe-ia {port | linkagg}**
  
  Displays the PPPoE-IA configuration for a physical port, physical port range, link aggregate port, or all the physical or link-aggregate ports.

- **show pppoe-ia statistics**
  
  Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

**MIB Objects**

- alaPPPoEIAGlobalRemoteIDFormatType
- alaPPPoEIAGlobalRemoteIDStringValue
clear pppoe-ia statistics

Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.

```
clear pppoe-ia statistics [port {chassis/slot/port[-port2] | linkagg agg_num]}
```

**Syntax Definitions**

- **chassis**: The chassis identifier.
- **slot**: The slot number for the module.
- **port**: Port number of the interface to be configured.
- **port2**: Last port number in a range of ports to be configured.
- **linkagg agg_num**: Specifies the link aggregate identification number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>6900</th>
<th>X48C4E/N48C8/</th>
<th>9900</th>
<th>X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X48C4E/N48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> clear pppoe-ia statistics
-> clear pppoe-ia statistics linkagg 13
```

**Release History**

Release 8.6R1; command introduced.
**Related Commands**

**pppoe-ia access-node-id**
Globally configures a format to form an identifier that uniquely identifies an access node.

**pppoe-ia circuit-id**
Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.

**show pppoe-ia statistics**
Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

**MIB Objects**

alaPPPoEIAGlobalClearStats
alaPPPoEIAStatsTable
  alaPPPoEIAStatsClearStats
show pppoe-ia configuration

Displays the global configuration for PPPoE-IA.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the Circuit-ID is configured with “default” parameter, then the Circuit-ID format will display as “ethernet”.
- If the Circuit-ID is configured with “default atm” parameter, then the Circuit-ID format will display as “atm”.

Examples

Default Configuration

-> pppoe-ia circuit-id default
-> show pppoe-ia configuration

Status : disabled,
Access Node Identifier
  Access-node-id Format : base-mac,
  Access-node-id String : 00:d0:95:ee:fb:02,
Circuit Identifier
  Circuit-Id Format : ethernet,
  Circuit-id Field1 : none,
  Circuit-id Field1 String : ,
  Circuit-id Field2 : none,
  Circuit-id Field2 String : ,
  Circuit-id Field3 : none,
  Circuit-id Field3 String : ,
  Circuit-id Field4 : none,
  Circuit-id Field4 String : ,
  Circuit-id Field5 : none,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter : ":",

...
Remote Identifier
   Remote-id Format : base-mac,
   Remote-id String : 00:d0:95:ee:fb:02
-> pppoe-ia circuit-id default atm
-> show pppoe-ia configuration
Status : enabled,
Access Node Identifier
   Access-node-id Format : base-mac,
   Access-node-id String : 00:d0:95:ee:fb:02,
Circuit Identifier
   Circuit-Id Format : atm,
   Circuit-id Field1 : none,
   Circuit-id Field1 String : ,
   Circuit-id Field2 : none,
   Circuit-id Field2 String : ,
   Circuit-id Field3 : none,
   Circuit-id Field3 String : ,
   Circuit-id Field4 : none,
   Circuit-id Field4 String : ,
   Circuit-id Field5 : none,
   Circuit-id Field5 String : ,
   Circuit-id Delimiter : ";",
Remote Identifier
   Remote-id Format : base-mac,
   Remote-id String : 00:d0:95:ee:fb:02

Output Definitions

<table>
<thead>
<tr>
<th>Status</th>
<th>Displays the global PPPoE-IA status: Enabled or Disabled.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-node-id Format</td>
<td>The format used to form an identifier that uniquely identifies an access node.</td>
</tr>
<tr>
<td>Access-node-id String</td>
<td>The value of user configured string for the access node.</td>
</tr>
<tr>
<td>Circuit-Id Format</td>
<td>The format used to form an identifier that uniquely identifies an access node and an access loop.</td>
</tr>
<tr>
<td>Circuit-id Field1</td>
<td>The Circuit-ID format.</td>
</tr>
<tr>
<td>Circuit-id Field1 String</td>
<td>The value of Circuit-ID depending on the format configured for the Circuit-ID.</td>
</tr>
<tr>
<td>Circuit-id Delimiter</td>
<td>A user configurable delimiter (a character) used to separate the fields of an ASCII string forming the Circuit-ID.</td>
</tr>
<tr>
<td>Remote-id Format</td>
<td>The format used to form an identifier that uniquely identifies the user attached to the access loop.</td>
</tr>
<tr>
<td>Remote-id String</td>
<td>The value of user configured string for the Remote-ID.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R1; command introduced.
**Related Commands**

- **pppoe-ia**
  Enable or disable PPPoE-IA globally on the switch.

- **pppoe-ia access-node-id**
  Globally configures a format to form an identifier that uniquely identifies an access node.

- **pppoe-ia circuit-id**
  Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.

- **pppoe-ia remote-id**
  Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.

- **show pppoe-ia statistics**
  Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

**MIB Objects**

- **alaPPPoEIAGlobalStatus**
- **alaPPPoEIAGlobalAccessNodeIDFormatType**
- **alaPPPoEIAGlobalAccessNodeIDStringValue**
- **alaPPPoEIAGlobalCircuitIDFormatType**
- **alaPPPoEIAGlobalCircuitIDField1**
- **alaPPPoEIAGlobalCircuitIDField1StrVal**
- **alaPPPoEIAGlobalCircuitIDField2**
- **alaPPPoEIAGlobalCircuitIDField2StrVal**
- **alaPPPoEIAGlobalCircuitIDField3**
- **alaPPPoEIAGlobalCircuitIDField3StrVal**
- **alaPPPoEIAGlobalCircuitIDField4**
- **alaPPPoEIAGlobalCircuitIDField4StrVal**
- **alaPPPoEIAGlobalCircuitIDField5**
- **alaPPPoEIAGlobalCircuitIDField5StrVal**
- **alaPPPoEIAGlobalCircuitIDDelimiter**
- **alaPPPoEIAGlobalRemoteIDFormatType**
- **alaPPPoEIAGlobalRemoteIDStringValue**
- **alaPPPoEIAGlobalClearStats**
show pppoe-ia {port | linkagg}

Displays the following:

- PPPoE-IA configuration for a physical or link-aggregate port, physical port range, or all the physical or link-aggregate ports.
- Port or port range configuration for ports with PPPoE-IA enabled or disabled
- Ports that are configured as trust or client port for PPPoE-IA.

```shell
class show pppoe-ia {port {chassis/lot/port[-port2] | linkagg agg_num} [enabled | disabled | trusted | client]
```

**Syntax Definitions**

- `chassis` The chassis identifier.
- `slot` The slot number for the module.
- `port` Port number of the interface to be configured.
- `port2` Last port number in a range of ports to be configured.
- `linkagg agg_num` Specifies the link aggregate identification number.
- `enabled` PPPoE-IA enabled port.
- `disable` PPPoE-IA disabled port.
- `trust` Port configured as trust.
- `client` Port configured as client.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A
Examples

Default Configuration
-> show pppoe-ia port
Chassis/Slot/Port   Status    Mode
----------+----------+------------
1/1/1     enabled     client
1/1/2     disabled    trusted
1/1/3     disabled    client
1/1/4     enabled     trusted
   ...
1/1/24    enabled     client
0/0       enabled     client
0/1       disabled    trusted

-> show pppoe-ia linkagg 1 enabled
ERROR: PPPoE-IA is disabled on linkagg 1

-> show pppoe-ia port 1/1/1 trusted
Chassis/Slot/Port   Status
----------+----------
1/1/1     enabled

-> show pppoe-ia port 1/1/1-5 client
Chassis/Slot/Port   Status
----------+----------
1/1/1     enabled
1/1/2     disabled
1/1/5     disabled

output definitions

<table>
<thead>
<tr>
<th>Chassis/Slot/Port</th>
<th>Status</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis, slot and port number.</td>
<td>PPPoE-IA enabled or disabled port.</td>
<td>Port configured as trust or client port for PPPoE-IA.</td>
</tr>
</tbody>
</table>

Release History

Release 8.6R1; command introduced.
**Related Commands**

**pppoe-ia**
Enable or disable PPPoE-IA globally on the switch.

**pppoe-ia {trust | client}**
Configures a port or a link aggregate port as trust or client port for PPPoE-IA.

**clear pppoe-ia statistics**
Cleans the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.

**show pppoe-ia configuration**
Displays the global configuration for PPPoE-IA.

**show pppoe-ia statistics**
Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

**MIB Objects**

- alaPPPoEIAGlobalStatus
- alaPPPoEIAGlobalAccessNodeIDFormatType
- alaPPPoEIAGlobalAccessNodeIDStringValue
- alaPPPoEIAGlobalCircuitIDFormatType
- alaPPPoEIAGlobalCircuitIDField1
- alaPPPoEIAGlobalCircuitIDField1StrVal
- alaPPPoEIAGlobalCircuitIDField2
- alaPPPoEIAGlobalCircuitIDField2StrVal
- alaPPPoEIAGlobalCircuitIDField3
- alaPPPoEIAGlobalCircuitIDField3StrVal
- alaPPPoEIAGlobalCircuitIDField4
- alaPPPoEIAGlobalCircuitIDField4StrVal
- alaPPPoEIAGlobalCircuitIDField5
- alaPPPoEIAGlobalCircuitIDField5StrVal
- alaPPPoEIAGlobalCircuitIDDelimiter
- alaPPPoEIAGlobalRemoteIDFormatType
- alaPPPoEIAGlobalRemoteIDStringValue
show pppoe-ia statistics

Displays the PPPoE-IA statistics for a physical port, link aggregate port, physical port range, or all the physical or link-aggregate ports.

show pppoe-ia \{port \{chassis/slot/port[-port2] | linkagg agg_num\} statistics

**Syntax Definitions**

- **chassis**
  - The chassis identifier.
- **slot**
  - The slot number for the module.
- **port**
  - Port number of the interface to be configured.
- **port2**
  - Last port number in a range of ports to be configured.
- **linkagg agg_num**
  - Specifies the link aggregate identification number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

**Default Configuration**

-> show pppoe-ia statistics

Chassis/

<table>
<thead>
<tr>
<th>Slot/</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
</tr>
<tr>
<td>1/1/2</td>
</tr>
<tr>
<td>1/1/24</td>
</tr>
<tr>
<td>0/0</td>
</tr>
<tr>
<td>0/1</td>
</tr>
</tbody>
</table>

-> show pppoe-ia linkagg 1 statistics

<table>
<thead>
<tr>
<th>Slot/</th>
</tr>
</thead>
<tbody>
<tr>
<td>0/1</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide  April 2023  page 56-23
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis/Slot/Port</td>
<td>Chassis, slot and port number.</td>
</tr>
<tr>
<td>PADI Rx</td>
<td>Valid PADI (PPPoE Active Discovery Initiation) packets received on the client port.</td>
</tr>
<tr>
<td>PADR Rx</td>
<td>Valid PADR (PPPoE Active Discovery Request) packets received on the client port.</td>
</tr>
<tr>
<td>PADT Rx</td>
<td>Valid PADT (PPPoE Active Discovery Terminate) packets received on the client port.</td>
</tr>
<tr>
<td>PADI Discard</td>
<td>Invalid (malformed or PDU length exceeds 1484) PADI packets received on the client port or no enabled trust port in the same VLAN as the client port.</td>
</tr>
<tr>
<td>PADR Discard</td>
<td>Invalid (malformed or PDU length exceeds 1500) PADR packets received on client port or no enabled trust port in the same VLAN as the client port.</td>
</tr>
<tr>
<td>PADT Discard</td>
<td>Invalid (malformed or PDU length exceeds 1500) PADT packets received on client port or no enabled trust port in the same VLAN as the client port.</td>
</tr>
<tr>
<td>PADO Discard</td>
<td>Total PADO (PPPoE Active Discovery Offer) packets received on the client port.</td>
</tr>
<tr>
<td>PADS Discard</td>
<td>Total PADS (PPPoE Active Discovery Session-confirmation) packets received on the client port.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- **pppoe-ia access-node-id**: Globally configures a format to form an identifier that uniquely identifies an access node.
- **pppoe-ia circuit-id**: Globally configures a Circuit-ID format that forms an identifier that uniquely identifies an access node and an access loop on which the PADI/PADR/PADT is received from the user side.
- **pppoe-ia remote-id**: Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.
- **clear pppoe-ia statistics**: Clears the statistics for all the physical or link-aggregate ports, a single port or a link aggregate port, or a range of physical ports for PPPoE-IA.
- **show pppoe-ia configuration**: Displays the global configuration for PPPoE-IA.
MIB Objects

alaPPPoEIAStatsTable
alaPPPoEIAStatsIfIndex
alaPPPoEIAStatsPADIRxCounter
alaPPPoEIAStatsPADRRxCounter
alaPPPoEIAStatsPADTRxCounter
alaPPPoEIAStatsPADIRxDiscardCounter
alaPPPoEIAStatsPADRRxDiscardCounter
alaPPPoEIAStatsPADTRxDiscardCounter
alaPPPoEIAStatsPADORxDiscardCounter
alaPPPoEIAStatsPADSRxDiscardCounter
Service Assurance Agent (SAA) enables customers to assure new business-critical applications, as well as services that utilize data, voice, and video. Use SAAs to verify service guarantees, increase network reliability by validating network performance, proactively identify network issues, and increase return on investment (ROI) by easing the deployment of new services. The SAA feature uses active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus enabling the measurement of network performance and health.

IP SAAs enhance the service level monitoring to become IP application-aware by measuring both end-to-end and at the IP layer. IP SAA would allow performance measurement against any IP addresses in the network (switch, server, pc). Use ETH-LB/DMM to measure delay and jitter by sending out frames with DM information to the peer MEP and receiving frames with DM information from the peer MEP.

MIB information for the SAA commands is as follows:

- **Filename:** Alcatel-IND1-ETHERNET-OAM-MIB.mib
  **Module:** alcatelIND1EoamMIB

- **Filename:** IEEE8021-CFM-MIB.mib
  **Module:** ieee8021CfmMib

- **Filename:** ALCATEL-IND1-SAA-MIB.mib
  **Module:** alcatelIND1SaaMIB

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>SAA Commands</th>
<th>saa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>saa start</td>
</tr>
<tr>
<td></td>
<td>saa stop</td>
</tr>
<tr>
<td></td>
<td>saa jitter-calculation enhanced</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EthOAM SAA Commands</th>
<th>saa type ethoam-loopback</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>saa type ethoam-two-way-delay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP SAA Command</th>
<th>saa type ip-ping</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Layer 2 SAA Command</th>
<th>saa type mac-ping</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>SPB SAA Commands</th>
<th>saa spb</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>saa spb reset</td>
</tr>
<tr>
<td></td>
<td>saa spb flush</td>
</tr>
<tr>
<td></td>
<td>show saa spb</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>XML SAA Commands</th>
<th>saa xml</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show saa xml</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SAA Show Commands</th>
<th>show saa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show saa type config</td>
</tr>
<tr>
<td></td>
<td>show saa statistics</td>
</tr>
<tr>
<td></td>
<td>show saa vrf</td>
</tr>
</tbody>
</table>
**saa**

Configures a Service Assurance Agent (SAA).

```
[vrf vrf_name] saa string [descr description] [interval interval] [jitter-threshold jitter_thresh] [rtt-threshold rtt_thresh]
```

```
[vrf vrf_name] no saa string
```

---

**Syntax Definitions**

- **vrf_name**
  The name of an existing VRF instance.

- **string**
  SAA ID string up to 32 characters. Use quotes around string if SAA ID contains multiple words with spaces between them (for example “SAA 10”).

- **description**
  Text string up to 32 characters. Use quotes around string if description contains multiple words with spaces between them (for example, “ALE Marketing SAA”).

- **interval**
  The amount of time, in minutes, between two iterations of the SAA test. Valid range is from 1, 2, 5, 10 to 1500.

- **jitter_thresh**
  The jitter threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.

- **rtt_thresh**
  The round-trip time threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>description</strong></td>
<td>DEFAULT</td>
</tr>
<tr>
<td><strong>interval</strong></td>
<td>150 minutes</td>
</tr>
<tr>
<td><strong>jitter_thresh</strong></td>
<td>0 (disabled)</td>
</tr>
<tr>
<td><strong>rtt_thresh</strong></td>
<td>0 (disabled)</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the **no** form of this command to remove an SAA from the switch configuration. Note that the SAA must be stopped before it can be deleted.
The desc and interval parameters are optional. If these values are specified, the SAA is created with those values. If these values are not specified, the SAA is created with the default values.

If the desc and/or interval parameters are specified for an existing SAA, then the values of the existing parameters are updated with those specified.

If the session time interval is changed for an SAA that is already running and active, the interval value is immediately updated in the database but is not applied to the SAA until after the next iteration.

If none of the optional parameters are specified and the given SAA exists, the CLI will return an error message, as duplicate entries are not allowed.

Any number of SAAs can be configured (MAX 127). It is recommended not to start many aggressive SAAs (having session interval <= 10). To achieve proper scheduling of all the started SAA (aggressive and relaxed) it is recommended not to start more than 50 SAAs.

Ensure the interval value is greater than the execution time (number of packets * inter packet delay).

When SAA processes an iteration of a session, it will compare the results against the following criteria to see if an SNMP trap should be sent. A trap with the session name is sent if:

- At least one packet is lost.
- Warning: Average RTT/Jitter crosses 90% of threshold.
- Critical: Average RTT/Jitter at or above threshold.

**Examples**

-> saa saa1 descr "saa for ip-ping"
-> saa saa1 jitter-threshold 100 rtt-threshold 500
-> saa saa2 descr "Monitoring Default VRF-interface" interval 160
-> saa saa2 interval 120
-> no saa saa1

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.2; jitter-threshold and rtt-threshold parameters added.

**Related Commands**

- show saa Displays SAA configuration information.
- show saa statistics Displays SAA statistics.

**MIB Objects**

alaSaaSaaCtrlTable
  alaSaaSaaCtrlTestIndex
  alaSaaSaaSaaCtrlRowStatus
  alaSaaSaaSaaCtrlDescr
  alaSaaSaaSaaCtrlInterval
  alaSaaSaaSaaCtrlJitterThreshold
  alaSaaSaaSaaCtrlRttThreshold
saa type ip-ping

Configure SAA for IP including the number of packets and inter-packet delay parameters.

```
[vrf vrf_name] saa string type ip-ping destination-ip ip_address source-ip ip_address type-of-service tos [num-pkts count] [inter-pkt-delay delay] [payload-size size]
```

### Syntax Definitions

- **vrf_name**
  The name of an existing VRF instance.

- **string**
  SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).

- **destination-ip ip_address**
  The IPv4 address of the destination to ping.

- **source-ip ip_address**
  The IPv4 address of the source.

- **tos ip_address**
  The type of service. Valid range is 0 – 255.

- **count**
  The number of packets to send in one ping iteration. The valid range is 1–100.

- **delay**
  The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100 ms to 1000 ms in multiples of 100 ms.

- **size**
  The size of the ICMP payload to be used for the ping iteration. Valid range is 24–1472 bytes.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>5</td>
</tr>
<tr>
<td>delay</td>
<td>1000 ms</td>
</tr>
<tr>
<td>size</td>
<td>24 bytes</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The **num-pkts**, **inter-pkt-delay**, and **payload-size** are optional parameters. If these values are specified, the SAA is created with the values entered. If none of them are specified, the SAA is created with the default values. The **num-pkts** and **inter-pkt-delay** can be modified, but **payload-size** cannot be modified later.
• Total execution time, that is, the product of num-pkts and inter-pkt-delay (number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.

• The SAA must not be in a ‘started’ state at the time the num-pkts or inter-pkt-delay parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.

• The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return an error.

• Do not specify a broadcast or multicast address for the source or destination IP. In addition, do not use 0.0.0.0 as the destination IP address.

• The timeout for each ping request packet is 1 sec. This value is not configurable.

• If a VRF is specified, the SAA for IP is configured in the specified VRF. By default, the SAA is configured in the ‘default’ VRF.

Examples

-> saa saa1 type ip-ping destination-ip 123.32.45.76 source-ip 123.35.42.124 type-of-service 4
-> saa saa2 type ip-ping destination-ip 123.32.45.77 source-ip 123.35.42.124 type-of-service 5
-> saa saa3 type ip-ping destination-ip 123.32.55.27 source-ip 123.35.42.125 type-of-service 8 inter-pkt-delay 1000
-> saa saa4 type ip-ping destination-ip 123.46.45.77 source-ip 123.35.42.125 type-of-service 2 num-pkts 5
-> saa saa5 type ip-ping destination-ip 12.53.45.77 source-ip 123.35.42.125 type-of-service 35 payload-size 1000
-> saa saa6 type ip-ping destination-ip 123.22.45.66 source-ip 123.35.42.125 type-of-service 5 inter-pkt-delay 1000 num-pkts 8 pkt-size 1000
-> vrf vrf3 saa saa7 type ip-ping destination-ip 123.22.45.66 source-ip 123.35.42.125 type-of-service 5 inter-pkt-delay 1000 num-pkts 8 pkt-size 1000

Release History
Release 7.3.1; command was introduced.

Related Commands

show saa Displays SAA configuration information.
show saa statistics Displays SAA statistics.

MIB Objects
alaSaaIpCtrlTable
  alaSaaIpCtrlTestIndex
  alaSaaIpCtrlRowStatus
  alaSaaIpCtrlTestMode
  alaSaaIpCtrlTgtAddress
  alaSaaIpCtrlSrcAddress
  alaSaaIpCtrlTypeOfService
  alaSaaIpCtrlInterPktDelay
  alaSaaIpCtrlPayloadSize
  alaSaaIpCtrlNumPkts
saa type mac-ping

Configure SAA for a MAC address including the VLAN, VLAN ID, number of packets and inter-packet delay parameters.

`saa string type mac-ping destination-mac mac_address vlan vlan_id [vlan-priority vlan_priority] [drop-eligible {true | false}] [data data] [num-pkts count] [inter-pkt-delay delay] [payload-size size] [isid-check isid]`

**Syntax Definitions**

- **string**: SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).
- **mac_address**: The destination MAC address to ping.
- **vlan_id**: The VLAN on which the L2 SAA Packets will be sent out. Valid range is 1-4094.
- **vlan_priority**: Specifies both the internal priority of the MAC ping and the 802.1p value on the VLAN tag header. Valid range is 0-7.
- **true**: Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to true.
- **false**: Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to false.
- **data**: User specified string to be included in the packet (Data TLV). Maximum string length for data is 255.
- **count**: The number of packets to send in one ping iteration. The valid range is 1–100.
- **delay**: The delay between packets sent during a ping iteration, in milliseconds. Valid range is from 100 ms to 1000 ms in multiples of 100 ms.
- **size**: The size of the ICMP payload to be used for the ping iteration. Valid range is 36–1500 bytes.
- **isid**: A service instance identifier (I-SID) that is used to identify the SPB service in a provider backbone bridge (PBB) network.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_priority</td>
<td>0</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>count</td>
<td>5</td>
</tr>
<tr>
<td>delay</td>
<td>1000 ms</td>
</tr>
<tr>
<td>size</td>
<td>36 bytes</td>
</tr>
</tbody>
</table>
Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The num-pkts, inter-pkt-delay, and payload-size are optional parameters. If these values are specified, the SAA is created with the values entered. If none of them are specified, the SAA is created with the default values. The num-pkts and inter-pkt-delay can be modified, but payload-size cannot be modified later.

- Total execution time, that is, the product of num-pkts and inter-pkt-delay (number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.

- The SAA must not be in a ‘started’ state at the time the num-pkts or inter-pkt-delay parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.

- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return an error.

- The timeout for each ping request packet is 1 sec. This value is not configurable.

- If data-TLV is specified and payload size is not specified, then payload size will be increased internally to accommodate the data TLV.

- If data TLV and payload size both are specified and payload size is less than [dataTLV + 36] bytes (for time-stamping and other packet info), then the CLI will be rejected.

- Destination-MAC cannot be broadcast/multicast address.

- Timeout for each ping request packet is 1 sec. This value is non-configurable.

- For SAA mac-ping over linkagg, it is recommended to have 5 (default) or more packets per session to ensure that accurate RTT and jitter values are obtained. Session iteration may see packet loss over linkagg if request and reply packets are not received on the same member port. This will not be seen in the subsequent iterations of the session.

Examples

- `saa saa1 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10`
- `saa saa4 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10 inter-pkt-delay 100`
- `saa saa5 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10 num-pkts 10`
- `saa saa6 type mac-ping destination-mac 00:11:11:11:11:11 vlan 10 payload-size 400`
- `saa saa8 type mac-ping destination-mac 00:11:11:11:11:11 vlan 1001 isid-check 1002`
Release History

Release 7.3.1; command was introduced.
Release 8.6R1; vlan-priority and drop-eligible parameters deprecated.

Related Commands

show saa Displays SAA configuration information.
show saa statistics Displays SAA statistics.

MIB Objects

alaSaaMacCtrlTable
  alaSaaMacCtrl1DstAddress
  alaSaaMacCtrl1Vlan
  alaSaaMacCtrl1VlanPriority
  alaSaaMacCtrl1PktData
  alaSaaMacCtrl1DropEligible
  alaSaaMacCtrl1PayloadSize
  alaSaaMacCtrl1NumPkts
  alaSaaMacCtrl1InterPktDelay
  alaSaaMacCtrl1Isid
**saa spb**

Configures session parameters for the Shortest Path Bridging (SPB) SAA. The SPB feature dynamically discovers SPB-enabled switches. Each discovered switch is identified by the pairing of a SPB VLAN (BVLAN) and the backbone MAC address (BMAC) for the switch. SPB advertises these BVLAN-BMAC pairs to the SAA feature, which in turn creates and starts MAC ping sessions based on the parameters configured with this command.

```
saa spb [auto-create] [auto-start] [interval interval] [vlan-priority vlan_priority] [drop-eligible {true | false}] ] [data data] [num-pkts count] [inter-pkt-delay delay] [payload-size size] [jitter-threshold jitter_thresh] [rtt-thresh rtt_thresh] [keep]
```

**Syntax Definitions**

- **auto-create**  
  Automatically creates an SPB SAA session for each discovered BVLAN-BMAC pair.

- **auto-start**  
  Automatically starts each SPB SAA session.

- **interval**  
  The amount of time, in minutes, between two iterations of the SAA test. Valid range is from 1, 2, 5, 10–1500.

- **vlan_priority**  
  Specifies both the internal priority of the MAC ping and the 802.1p value on the VLAN tag header. Valid range is 0-7.

- **true**  
  Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to true.

- **false**  
  Sets both the internal drop precedence of the MAC ping and the CFI bit on the VLAN tag header to false.

- **data**  
  User specified string to be included in the packet (Data TLV). Maximum string length for data is 255.

- **count**  
  The number of packets to send in one ping iteration of the test. Valid range is 1–100.

- **delay**  
  The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100–1000 ms in multiples of 100 ms.

- **size**  
  The size of the ICMP payload to be used for the ping iteration. Valid range is 32–1500 bytes.

- **jitter_thresh**  
  The jitter threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.

- **rtt_thresh**  
  The round-trip time threshold value, in microseconds. A trap is generated when this value is crossed. The valid range is 0–1000000.

- **keep**  
  Retains SPB SAA session information even when SPB signals that a BMAC or BVLAN no longer exists.
Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-create</td>
<td>off</td>
</tr>
<tr>
<td>auto-start</td>
<td>off</td>
</tr>
<tr>
<td>interval</td>
<td>150 minutes</td>
</tr>
<tr>
<td>vlan-priority</td>
<td>0</td>
</tr>
<tr>
<td>drop-eligible {true</td>
<td>false}</td>
</tr>
<tr>
<td>data</td>
<td>null</td>
</tr>
<tr>
<td>count</td>
<td>5</td>
</tr>
<tr>
<td>delay</td>
<td>1000 ms</td>
</tr>
<tr>
<td>size</td>
<td>32 bytes</td>
</tr>
<tr>
<td>jitter_thresh</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>rtt-thresh</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>keep</td>
<td>off</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The **auto-create** and **auto-start** parameters enable the SPB SAA functionality required to automatically create and start this type of SAA session.

- Ensure the interval value is greater than the execution time (number of packets * inter-packet delay).

- Total execution time, that is, the product of **num-pkts** and **inter-pkt-delay** (number of packets * inter-packet delay) for an SAA iteration must be less than the sum of interval and inter-packet delay.

- SPB SAA sessions cannot be modified but are automatically configured with “SPB” as the owner of the session so they can be easily identified within the applicable SAA **show** command displays.

- The SAA ID for an SPB SAA is the prefix SPB- combined with the BVLAN and BMAC pairing used to generate the session. For example, SPB-bvlan-bmac (SPB-4000-e8-e7-32-07-98-cd).

- For SAA mac-ping over linkagg, it is recommended to have 5 (default) or more packets per session to ensure that accurate RTT and jitter values are obtained. Session iteration may see packet loss over linkagg if request and reply packets are not received on the same member port. This will not be seen in the subsequent iterations of the session.
Examples

-> saa spb auto-create auto-start interval 160 num-pkts 50 inter-pkt-delay 100 keep
-> saa spb auto-create auto-start jitter-threshold 100 rtt-threshold 500
-> saa spb keep

Release History

Release 7.3.2; command was introduced.
Release 8.6R1; vlan-priority and drop-eligible parameters deprecated.

Related Commands

show saa spb
saa spb flush
saa spb reset

MIB Objects

alaSaaSpbFeature
alaSaaSpbAutoCreate
alaSaaSpbAutoStart
alaSaaSpbInterval
alaSaaSpbVlanPriority
alaSaaSpbDropEligible
alaSaaSpbPktData
alaSaaSpbNumPkts
alaSaaSpbInterPktDelay
alaSaaSpbPayloadSize
alaSaaSpbJitterThreshold
alaSaaSpbRTTThreshold
alaSaaSpbKeep
**saa spb reset**

Resets all of the SPB SAA session parameters to their default values.

```plaintext
saa spb reset
```

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When this command is used, the SPB SAA session parameters are set to the following default values:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto-create</td>
<td>off</td>
</tr>
<tr>
<td>auto-start</td>
<td>off</td>
</tr>
<tr>
<td>interval</td>
<td>150 minutes</td>
</tr>
<tr>
<td>vlan-priority</td>
<td>0</td>
</tr>
<tr>
<td>drop-eligible</td>
<td>false</td>
</tr>
<tr>
<td>data</td>
<td>null</td>
</tr>
<tr>
<td>count</td>
<td>5</td>
</tr>
<tr>
<td>delay</td>
<td>1000 ms</td>
</tr>
<tr>
<td>size</td>
<td>32 bytes</td>
</tr>
<tr>
<td>jitter_thresh</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>rtt-thresh</td>
<td>0 (disabled)</td>
</tr>
<tr>
<td>keep</td>
<td>off</td>
</tr>
</tbody>
</table>

**Examples**

```
-> saa spb reset
```
Release History
Release 7.3.2; command was introduced.
Release 8.6R1; vlan-priority and drop-eligible parameters deprecated.

Related Commands
- **show saa spb**  
  Displays the SAA configuration for the SPB SAA.
- **saa spb flush**  
  Clears all SPB SAA sessions and rebuilds the sessions based on the information learned from SPB.
- **saa spb**  
  Configures SPB SAA session parameters.

MIB Objects
- **alaSaaSpbFeature**
- **alaSaaSpbReset**
saa spb flush

Cleans all SPB SAA sessions and rebuilds the sessions based on the information learned from SPB.

saa spb flush

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command does not stop the automatic creation or start of SPB sessions or change any of the SPB SAA session parameters.

**Examples**

```
-> saa spb flush
```

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

- `show saa spb` Displays SAA configuration information.
- `saa spb reset` Resets all SPB SAA session parameters back to their default values.
- `saa spb` Configures SPB SAA session parameters.

**MIB Objects**

- `alaSaaSpbFeature`
- `alaSaaSpbReset`
**saa type ethoam-loopback**

Configures the SAA for ETH-LB, including the number of packets and inter-packet delay parameters.

\[
\text{saa string type ethoam-loopback \{target-endpoint t_mepid | target-mac address mac_address\} source-endpoint s_mepid domain md_name association ma_name vlan-priority vlan_priority [drop-eligible \{true | false\}] [data data] [num-pkts num] [inter-pkt-delay delay]}
\]

### Syntax Definitions

<table>
<thead>
<tr>
<th>string</th>
<th>SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).</th>
</tr>
</thead>
<tbody>
<tr>
<td>t_mepid</td>
<td>The ID of the destination MEP.</td>
</tr>
<tr>
<td>mac_address</td>
<td>The MAC address of the destination.</td>
</tr>
<tr>
<td>s_mepid</td>
<td>The ID of the source MEP.</td>
</tr>
<tr>
<td>md_name</td>
<td>The domain to which the source MEP belongs.</td>
</tr>
<tr>
<td>ma_name</td>
<td>The association to which the source MEP belongs.</td>
</tr>
<tr>
<td>vlan_priority</td>
<td>The VLAN priority to be used for the outgoing packet. The valid range is 0-7.</td>
</tr>
<tr>
<td>true</td>
<td>Sets the drop eligibility bit in the VLAN tag to true.</td>
</tr>
<tr>
<td>false</td>
<td>Sets the drop eligibility bit in the VLAN tag to false.</td>
</tr>
<tr>
<td>data</td>
<td>User specified string that is included in the packet. Maximum string length for data is 255.</td>
</tr>
<tr>
<td>num</td>
<td>The number of packets to send during loopback. Valid range is 1–100.</td>
</tr>
<tr>
<td>delay</td>
<td>The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100–1000 ms in multiples of 100 ms.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop-eligible {true</td>
<td>false}</td>
</tr>
<tr>
<td>num-pkts num</td>
<td>5</td>
</tr>
<tr>
<td>delay</td>
<td>1000</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 57-15
Usage Guidelines

- The SAA must exist before issuing the CLI. If the SAA does not exist, the CLI will return error.
- Source MEP-ID, MD and MA must be created before initiating loopback.
- If the source MEP-Id/MA/MD does not exist, the configuration will be accepted and no error will be returned.
- When target-endpoint is specified then it must be learned before initiating loopback.
- When target-endpoint is specified and learned, Ethernet Loopback will be transmitted irrespective of whether the RMEP state is OK or failed.
- The data, num-pkts, and inter-pkt-delay are optional parameters. If these values are specified, the entry will be created with these values. If none of them are specified, the SAA will be created with default values. The num-pkts and inter-pkt-delay can be modified later.
- Total execution time, that is, the product of num-pkts and inter-pkt-delay (number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.
- The SAA must not be in a ‘started’ state at the time the num-pkts or inter-pkt-delay parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.
- The Target MEP/MAC, source MEP, domain, and association parameters are mandatory. If they are not specified, the CLI will return an error.
- The data parameter is optional. If this parameter is not specified, then it is not sent in the loopback message.
- The timeout value for each LB packet is one second. This value is not configurable.
- For SAA Ethernet OAM over linkagg, it is recommended to have 5 (default) or more packets per session to ensure that accurate RTT and jitter values are obtained.

Examples

- `saa saa1 type ethoam-loopback target-endpoint 10 source endpoint 1 domain md1 association ma1`
- `saa saa2 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1 association ma1 data "monitor association ma1" num-pkts 6 inter-pkt-delay 500`
- `saa saa3 type ethoam-loopback target-endpoint 15 source endpoint 1 domain md1 association ma1 data "monitor association ma1" num-pkts 6`
- `saa saa4 type ethoam-loopback target-endpoint 10 source endpoint 2 domain md1 association ma1 inter-pkt-delay 500`

Release History

Release 7.3.1; command was introduced.
Release 8.6R1; vlan-priority and drop-eligible parameters deprecated.
Related Commands

```
show saa
``` Displays SAA configuration information.

```
show saa statistics
``` Displays SAA statistics.

MIB Objects

```
alaSaaEthoamCtrlTable
  alaSaaEthoamCtrlTestIndex
  alaSaaEthoamCtrlRowStatus
  alaSaaEthoamCtrlTestMode
  alaSaaEthoamCtrlTgtMAC
  alaSaaEthoamCtrlSrcMepId
  alaSaaEthoamCtrlDomainName
  alaSaaEthoamCtrlAssociationName
  alaSaaEthoamCtrlNumPkts
  alaSaaEthoamCtrlInterPktDelay
  alaSaaEthoamCtrlPktData
  alaSaaEthoamCtrlVlanPriority
```
**saa type ethoam-two-way-delay**

Configuration SAA for ETH-DMM, including the number of packets and inter-packet delay parameters.

```
saa string type {ethoam-two-way-delay} {target-endpoint t_mepid | target-mac address mac_address}
source-endpoint s_mepid domain md_name association ma_name vlan-priority vlan_priority [num-pkts num] [inter-pkt-delay delay]
```

**Syntax Definitions**

- **string**  
  SAA ID string up to 32 characters. Use quotes around string if the SAA ID contains multiple words with spaces between them (for example, “SAA 10”).

- **t_mepid**  
  The ID of the destination MEP.

- **mac_address**  
  The MAC address of the destination.

- **s_mepid**  
  The ID of the source MEP.

- **md_name**  
  The domain to which the source MEP belongs.

- **ma_name**  
  The association to which the source MEP belongs.

- **vlan_priority**  
  The VLAN priority to be used for the outgoing packet. The valid range is 0-7.

- **num**  
  The number of packets to send during loopback. Valid range is 1–100.

- **delay**  
  The delay between packets sent during a ping iteration, in milliseconds. Valid range is 100–1000 ms in multiples of 100 ms.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>num</td>
<td>5</td>
</tr>
<tr>
<td>delay</td>
<td>1000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The SAA should exist before issuing the CLI. If the SAA does not exist, the CLI will return error.
- The source MEP-ID, MD, and MA must be created before initiating DMM.
• If the source MEP-Id/MA/MD does not exist, the configuration will be accepted and no error will be returned.

• When the target-endpoint parameter is specified, then it must be learned before initiating DMM.

• When the target-endpoint parameter is specified and learned, ETH-DMM will be transmitted irrespective of whether the RMEP state is OK or failed.

• The num-pkts and inter-pkt-delay parameters are optional. If these values are specified, the entry will be created with those values. If none of them are specified, the SAA will be created with default values. The num-pkts and inter-pkt-delay values can be modified, but the pkt-size value cannot be modified later.

• Total execution time, that is, the product of num-pkts and inter-pkt-delay (number of packets * inter-packet delay) for a SAA iteration must be less than the sum of interval and inter-packet delay.

• The SAA must not be in a ‘started’ state at the time the num-pkts or inter-pkt-delay parameters are modified. Make sure the SAA is stopped before attempting to modify these parameters.

• Target MEP/MAC, source MEP, domain, and association parameters are mandatory. If they are not specified, the CLI will return an error.

• The timeout for each DMM packet is 1 sec. This value is not configurable.

• For SAA Ethernet OAM over linkagg, it is recommended to have 5 (default) or more packets per session to ensure that accurate RTT and jitter values are obtained.

Examples

-> saa saa1 type ethoam-two-way-delay target-endpoint 10 source endpoint 1 domain md1 association ma1
-> saa saa2 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain md1 association ma1 num-pkts 6 inter-pkt-delay 500
-> saa saa3 type ethoam-two-way-delay target-endpoint 15 source endpoint 1 domain md1 association ma1 num-pkts 6
-> saa saa4 type ethoam-two-way-delay target-endpoint 10 source endpoint 2 domain md1 association ma1 inter-pkt-delay 500

Release History

Release 7.3.1; command was introduced.
Release 8.6R1; vlan-priority parameter deprecated.
Related Commands

- **show saa**
  Displays SAA configuration information.
- **show saa statistics**
  Displays SAA statistics.

MIB Objects

alaSaaEthoamCtrlTable
  - alaSaaEthoamCtrlTestIndex
  - alaSaaEthoamCtrlRowStatus
  - alaSaaEthoamCtrlTestMode
  - alaSaaEthoamCtrlTgtMAC
  - alaSaaEthoamCtrlSrcMepId
  - alaSaaEthoamCtrlDomainName
  - alaSaaEthoamCtrlAssociationName
  - alaSaaEthoamCtrlNumPkts
  - alaSaaEthoamCtrlInterPktDelay
  - alaSaaEthoamCtrlVlanPriority
saa start

Starts the SAA test.

[vrf vrf_name] saa string start [at yyyy-mm-dd,hh:mm:ss]

Syntax Definitions

vrf_name The name of an existing VRF instance.
string An existing SAA ID string.
yyyy-mm-dd,hh:mm:ss The date and time to start the SAA.

Defaults

By default, the SAA test is started immediately.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- An existing SAA with the SAA type configured must be specified with this command.
- Use the saa stop command to stop an SAA test that is already running.
- Use the at option to specify a date and time for the test to start.
- If an SAA is scheduled to start at a specified time and another saa start command with a different value is given before the specified time, the subsequent command will over-ride the previous command.
- If the saa start command is given after an SAA is started, then the CLI will return error.
- If the SAA type is configured with a source IP that does not exist or is not active, then the packet will not be transmitted and no error will be returned. Swlogs will be updated.
- ICMP must be enabled on the switch. If ICMP is disabled and an SAA of type 'ip-ping’ is started, then the iteration will timeout and will be treated as failed iteration.
- Immediately after a CMM restart (reboot or takeover), the command to start SAA will be accepted, but the actual execution of the iteration will start 5 minutes after the CMM restart.
- If the SAA type is configured with a source MEP that does not exist or is not active (admin down), then the packet will not be transmitted and no error will be returned on the CLI console. Swlogs will be updated.
• It is recommended that all the SAAs be rescheduled if the system time is being changed.

Examples

-> saa saa2 start at 2009-09-12,09:00:00
-> saa saa4 start

Release History

Release 7.3.1; command was introduced.

Related Commands

show saa
  Displays SAA configuration information.

show saa statistics
  Displays SAA statistics.

MIB Objects

alaSaaCtrlTable
  alaSaaCtrlTestIndex
  alaSaaCtrlStartAt
**saa stop**

Stops the SAA test.

```
[vrf vrf_name] saa string stop [never | at yyyy-mm-dd,hh:mm:ss]
```

### Syntax Definitions

- **vrf_name**
  - The name of an existing VRF instance.

- **string**
  - An existing SAA ID string.

- **never**
  - Specifies that the SAA test will not be stopped unless the **saa stop** command is used with the **at** option.

- **yyyy-mm-dd,hh:mm:ss**
  - The date and time to start the SAA.

### Defaults

By default, the test is stopped immediately.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- An existing SAA with the SAA type configured must be specified with this command.
- The SAA must be in a ‘started’ state before giving the command unless the start and stop times are scheduled. If the SAA is not in a ‘started’ state, the CLI will return an error.
- Use the **at** option to specify a date and time for the test to stop.
- If the **never** option is specified, the SAA test will keep on running until the **saa stop** command is entered again with the **at** option.
- If SAA test is stopped while it is running an iteration, the current iteration is pre-empted. The statistics and history are updated for the partial iteration run.
- If an SAA is scheduled to stop at a specified time and another **saa stop** command with a different value is given before the specified time, the subsequent command will over-ride the previous command.

### Examples

```
-> saa saa1 stop
-> saa saa2 stop never
```
**Release History**

Release 7.3.1; command was introduced.

**Related Commands**

- `show saa` Displays SAA configuration information.
- `show saa statistics` Displays SAA statistics.

**MIB Objects**

- `alaSaaCtrlTable`
  - `alaSaaCtrlTestIndex`
  - `alaSaaCtrlStopAt`
saa jitter-calculation enhanced

Calculates jitter values on each SAA probe. Each and every jitter that is calculated will be implemented as per the formula specified in RFC 1889.

Syntax Definitions

N/A

Defaults

By default, the inter-arrival jitter calculation is based on the round-trip-time difference between two successive packets.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When the jitter calculation mode is set to enhanced, then jitter calculation will be made as per RFC 1889 defined formula.

  Formula:
  
  Jitter = Jitter + (abs (ElapsedTime - OldElapsedTime ) - Jitter) / 16

  Where
  
  ‘Jitter’ - Jitter value calculated from successive packets RTT.
  Elapsed - RTT value involved in the packet.

- The jitter calculation is applicable for IP SAA, ETH SAA, MAC SAA, and SAA SPB.

- The enhanced jitter calculation will only affect the jitter calculation for the overall iteration. The calculation of jitter for individual packets will not change with enhanced mode.

- Use the no form of this command to set the jitter calculation to default.

Examples

- saa jitter-calculation enhanced

- no saa jitter-calculation enhanced
**Release History**

Release 8.8R1; command introduced.

**Related Commands**

*show saa* Displays the mode which is set for jitter calculation.

**MIB Objects**

alaSaaJitterCalculationConfigGroup
alaSaaJitterCalculationEnhanced
**saa xml**

Configures SAA XML parameters that determine when and where an SAA XML history file is created.

```
saa xml [file-name xml_filename] [interval interval] [admin-state {enable | disable}]
```

**Syntax Definitions**

- `xml_filename` The name of the file where SAA history entries are stored. This file must reside in the `/flash/network` directory on the local switch.
- `interval` The amount of time, in minutes, between each generation of the XML history file. Valid range is from 1–15000.
- `enable` Enables XML history file generation.
- `disable` Disables XML history file generation.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>xml_filename</code></td>
<td>saa.xml</td>
</tr>
<tr>
<td><code>interval</code></td>
<td>20 minutes</td>
</tr>
<tr>
<td><code>admin-state</code></td>
<td>Disabled</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

- When this function is enabled, SAA will periodically generate an XML file containing the following entries:
  - SAA name and ID
  - VRF name
  - Iteration number (1-5)
  - Last run time
  - Reason
  - Packets sent/received
  - InterPktDelay
  - EgressPort
  - RTT min/avg/max (value is ‘-1’ in case of failed test)
  - Jitter min/avg/max (value is ‘-1’ in case of failed test)
  - Subports

**Examples**

-> saa xml interval 60 admin-state enable
-> saa xml file-name switch1_saa.xml interval 120 admin-status enable

**Release History**

Release 7.3.2; command was introduced.

**Related Commands**

*show saa xml* Displays the SAA XML file generation parameters.

**MIB Objects**

alaSaaXmlFeature
alaSaaXmlStatus
alaSaaXmlFilename
alaSaaXmlInterval
show saa

Displays SAA session information.

[vrf vrf_name] show saa [string | {descr description}] | [owner saa_owner]

**Syntax Definitions**

- **vrf_name**: The name of an existing VRF instance.
- **string**: An existing SAA ID.
- **description**: An existing SAA description string.
- **saa_owner**: The owner name associated with the SAA session.

**Defaults**

By default, information is displayed for all SAA sessions.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **string** or **descr description** parameter to display information for a specific SAA.
- Use the **owner saa_owner** parameter to display only those sessions initiated by a specific owner. The owner of an SAA session is not user configurable, but identifies the entity that created the session.
- When an SAA is created, an owner name is assigned to the agent. This name is based on the Alcatel-Lucent Enterprise application that generated the SAA and is not configurable. For example:
  - CLI SAA owner name = “USER”
  - OmniVista owner name = “OV”
  - Shortest Path Bridging owner name = “SPB” (SAA ID is SPB-bvlan-bmac)

**Examples**

```
-> show saa
Legend: eth-lb = ethoam-loopback
       eth-dmm = ethoam-two-way-delay
       jitter-calculation = Default

SAA                      Owner Type Status Interval Time of Last Run Last Run Description
--------------------------+-----+--------+------+-----+---------------------+-------+--------
SPB-4000-e8-e7-32-07-98-cd  SPB  mac-ping started   1 2013-03-06,18:01:35.0 success DEFAULT
Saa20                   USER ip-ping started 130 2013-01-15,09:31:53.0 success DEFAULT
```
Service Assurance Agent Commands

show saa

- saa31 USER ip-ping started 180 2013-01-12,21:30:05.0 failed DC1
- saa90 USER eth-lb stopped 150 NOT RUN undetermined DC5
- saa95 USER eth-lb stopped 300 2013-01-6,11:31:53.0 success EthLB

-> show saa SPB-4000-e8-e7-32-07-98-cd owner spb

Legend: eth-lb = ethoam-loopback
eth-dmm = ethoam-two-way-delay

<table>
<thead>
<tr>
<th>SAA</th>
<th>Owner Type</th>
<th>Type</th>
<th>Status</th>
<th>Interval (min)</th>
<th>Time of Last Run</th>
<th>Last Run Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPB-4000-e8-e7-32-07-98-cd</td>
<td>SPB</td>
<td>mac-ping</td>
<td>started</td>
<td>1</td>
<td>2013-03-06,18:01:35.0</td>
<td>success</td>
<td>DEFAULT</td>
</tr>
</tbody>
</table>

-> vrf vrf3 show saa

<table>
<thead>
<tr>
<th>SAA</th>
<th>Owner Type</th>
<th>Type</th>
<th>Status</th>
<th>Interval (min)</th>
<th>Time of Last Run</th>
<th>Last Run Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPB-4000-e8-e7-32-07-98-cd</td>
<td>SPB</td>
<td>mac-ping</td>
<td>started</td>
<td>1</td>
<td>2013-03-06,18:01:35.0</td>
<td>success</td>
<td>DEFAULT</td>
</tr>
</tbody>
</table>

output definitions

- **SAA**: SAA name.
- **Owner Type**: The owner name assigned to the agent.
- **Type**: The SAA type.
- **Status**: The status of the SAA test: started or stopped.
- **Interval (min)**: The amount of time between two iterations of the SAA test.
- **Time of Last Run**: The time the SAA was last run.
- **Last Run Result**: Result of last iteration.
- **Description**: Configured description for the SAA.

Release History

- Release 7.3.1; command was introduced.
- Release 7.3.2; owner parameter and field added.
- Release 8.8R1; Jitter-calculation field added.

Related Commands

- **saa**: Configures an SAA.

MIB Objects

- **alaSaaCtrlTable**
  - **alaSaaCtrlOwnerIndex**
  - **alaSaaCtrlTestIndex**
  - **alaSaaCtrlDescr**
  - **alaSaaCtrlInterval**
  - **alaSaaCtrlTestMode**
  - **alaSaaCtrlLastRunTime**
  - **alaSaaCtrlLastRunResult**
  - **alaSaaCtrlAdminStatus**
show saa type config

Displays the SAA configuration for the specified SAA type.

```
[vrf vrf_name] show saa [string] type {mac-ping | ip-ping | ethoam-loopback | ethoam-two-way-delay} config
```

Syntax Definitions

- **vrf_name**: The name of an existing VRF instance.
- **string**: An existing SAA ID.
- **mac-ping**: Displays MAC Ping SAAs.
- **ip-ping**: Displays IP Ping SAAs.
- **ethoam-loopback**: Displays ETH-LB SAAs.
- **ethoam-two-way-delay**: Displays ETH-DMM SAAs.

Defaults

By default, all SAAs with the specified type are displayed.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the `string` parameter to display information for a specific SAA.
- If the SAA ID string specified does not match the specified SAA type, the CLI will return an error.
- If a specific VRF is specified, the IP ping sessions for that VRF is displayed.

Examples

```
-> show saa type ip-ping config
SAA : saa20
  SAA-type : ip-ping,
  Status    : started,
  Start At  : -
  Stop At   : 2010-02-08,12:00:00.0
  Description: datacenter1,
  Interval(minutes) : 130,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms) : 0,
  Source-IP  : 0.0.0.0,
```
Service Assurance Agent Commands

show saa type config

Destination-IP : 172.21.161.65,
Payload-Size (bytes) : 24,
Type-of-Service : 0,
Num-pkts : 5,
Inter-pkt-delay : 1000
SAA : saa31
  SAA-type : ip-ping,
  Status : started,
  Start At : -
  Stop At : -
  Description : datacenter8,
  Interval(minutes) : 180,
  Jitter Threshold (ms) : 100,
  RTT Threshold (ms) : 500,
  Source-IP : 0.0.0.0,
  Destination-IP : 172.21.161.65,
  Payload-Size (bytes) : 24,
  Type-of-Service : 0,
  Num-pkts : 5,
  Inter-pkt-delay : 1000

-> vrf vrf3 show saa type ip-ping config
SAA : saa1,
  SAA-type : ip-ping,
  Status : stopped,
  Start At : -
  Stop At : -
  Description : DEFAULT,
  Interval(minutes) : 150,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms) : 0,
  Source-IP : 2.2.2.2,
  Destination-IP : 1.1.1.1,
  Payload-Size (bytes) : 24,
  Type-of-Service : 2,
  Num-pkts : 5,
  Inter-pkt-delay : 1000

SAA : saa2,
  SAA-type : ip-ping,
  Status : stopped,
  Start At : -
  Stop At : -
  Description : DEFAULT,
  Interval(minutes) : 150,
  Jitter Threshold (ms) : 0,
  RTT Threshold (ms) : 0,
  Source-IP : 2.2.2.2,
  Destination-IP : 1.1.1.1,
  Payload-Size (bytes) : 24,
  Type-of-Service : 4,
  Num-pkts : 5,
  Inter-pkt-delay : 1000

-> show saa type ethoam-loopback config
Legend: Destination Mep: - = SAA configured with target mac-address
        Destination MAC: - = SAA configured with target mep-id
SAA : saa90
  SAA-type : ethoam-loopback,
show saa type config

SAA : saa99
   SAA-type  : ethoam-loopback,
   Status    : started,
   Description: SAA for ethernet-loopback,
   Interval(minutes) : 300,
   Jitter Threshold (ms) : 0,
   RTT Threshold (ms) : 0,
   Target-MAC : -,
   Target-Endpoint : 5,
   Source-Endpoint : 1,
   Domain       : ale,
   Association  : ma1,
   Num-pkts     : 7,
   Inter-pkt-delay : 1000,
   Data         : ""

SAA : saa100
   SAA-type  : ethoam-two-way-delay,
   Status    : stopped,
   Description: SAA for ethernet-two-way-test,
   Interval(minutes) : 200,
   Jitter Threshold (ms) : 0,
   RTT Threshold (ms) : 0,
   Target-MAC : 00:d0:b2:12:3c:a5,
   Target-Endpoint : -,
   Source-Endpoint : 4,
   Domain       : aricent
   Association  : ma1,
   Num-pkts     : 5,
   Inter-pkt-delay : 500

SAA : saa110
   SAA-type  : ethoam-two-way-delay,
   Status    : started,
   Description: SAA for ethernet-two-way-delay,
   Interval(minutes) : 300,
   Jitter Threshold (ms) : 0,
   RTT Threshold (ms) : 0,
   Target-MAC : -,
   Target-Endpoint : 5,
   Source-Endpoint : 1,
   Domain       : aricent,
   Association  : ma2,
   Num-pkts     : 7,
   Inter-pkt-delay : 800

Legend: Destination MEP: - = SAA configured with target mac-address
         Destination MAC: - = SAA configured with target mep-id
Service Assurance Agent Commands

show saa type config

output definitions

<table>
<thead>
<tr>
<th>SAA-type</th>
<th>Type of SAA entry.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status of the SAA test.</td>
</tr>
<tr>
<td>Start At</td>
<td>Start time of the SAA test.</td>
</tr>
<tr>
<td>Stop At</td>
<td>Stop time of the SAA test.</td>
</tr>
<tr>
<td>Description</td>
<td>Configured description for the SAA.</td>
</tr>
<tr>
<td>Jitter Threshold (ms)</td>
<td>The configured jitter threshold value, in microseconds.</td>
</tr>
<tr>
<td>RTT Threshold (ms)</td>
<td>The configured round-trip time threshold value, in microseconds.</td>
</tr>
<tr>
<td>Source-IP</td>
<td>The IPv4 address of the source.</td>
</tr>
<tr>
<td>Destination-IP</td>
<td>The IPv4 address of the destination.</td>
</tr>
<tr>
<td>Payload-Size (bytes)</td>
<td>Size of ICMP payload for the packet.</td>
</tr>
<tr>
<td>Type-of-Service</td>
<td>Type of service.</td>
</tr>
<tr>
<td>Target-MAC</td>
<td>The target MAC address of the destination.</td>
</tr>
<tr>
<td>Target-Endpoint</td>
<td>The ID of the destination MEP.</td>
</tr>
<tr>
<td>Source-Endpoint</td>
<td>The ID of the source MEP.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain to which the source MEP belongs.</td>
</tr>
<tr>
<td>Association</td>
<td>The association to which the source MEP belongs.</td>
</tr>
<tr>
<td>Num-pkts</td>
<td>Number of packets per iteration.</td>
</tr>
<tr>
<td>Inter-pkt-delay</td>
<td>Delay between two consecutive packets.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.1; command was introduced.
Release 7.3.2; Jitter Threshold and RTT Threshold fields added.

Related Commands

saa type mac-ping Configures a MAC ping SAA.
saa type ip-ping Configures an IP ping SAA.
saa type ethoam-loopback Configures an ETH-LB SAA.
saa type ethoam-two-way-delay Configures an ETH-DMM SAA.
**MIB Objects**

alaSaaCtrlTable
alaSaaCtrlTestIndex
alaSaaCtrlDescr
alaSaaCtrlInterval
alaSaaCtrlTestMode
alaSaaCtrlJitterThreshold
alaSaaCtrlRTTThreshold
alaSaaMacCtrlTable
alaSaaMacCtrlDstAddress
alaSaaMacCtrlPayloadSize
alaSaaMacCtrlInterPktDelay
alaSaaMacCtrlNumPkts
alaSaaIpCtrlTable
alaSaaIpCtrlTgtAddress
alaSaaIpCtrlSrcAddress
alaSaaIpCtrlPayloadSize
alaSaaIpCtrlTypeOfService
alaSaaIpCtrlInterPktDelay
alaSaaIpCtrlNumPkts
alaSaaEthoamCtrlTable
alaSaaEthoamCtrlTestMode
alaSaaEthoamCtrlAdminStatus
alaSaaEthoamCtrlTgtMepId
alaSaaEthoamCtrlTgtMAC
alaSaaEthoamCtrlSrcMepId
alaSaaEthoamCtrlInterPktDelay
**show saa spb**

Displays the SAA configuration for the Shortest Path Bridging (SPB) SAA.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the SAA parameters that are applied to SPB SAA sessions. Use the `show saa` command to get specific session status and information.

**Examples**

`-> show saa spb`

**output definitions**

**Auto-create**

Displays if SPB SAA functionality required to automatically create the SAA session is enabled or disabled.

**Auto-start**

Displays if SPB SAA functionality required to automatically start the SAA session is enabled or disabled.
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval (minutes)</td>
<td>The amount of time between two iterations of the SAA test.</td>
</tr>
<tr>
<td>Jitter Threshold (ms)</td>
<td>The configured jitter threshold value, in microseconds.</td>
</tr>
<tr>
<td>RTT Threshold (ms)</td>
<td>The configured round-trip time threshold value, in microseconds.</td>
</tr>
<tr>
<td>Payload-Size (bytes)</td>
<td>Size of ICMP payload.</td>
</tr>
<tr>
<td>Num-pkts</td>
<td>Number of packets per iteration</td>
</tr>
<tr>
<td>Inter-pkt-delay</td>
<td>Delay between two consecutive packets.</td>
</tr>
<tr>
<td>Keep</td>
<td>Displays if SPB SAA session information must be retained or not even when SPB signals that a BMAC or BVLAN no longer exists.</td>
</tr>
<tr>
<td>Data</td>
<td>DataUser specified string that is included in the packet.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.2; command was introduced.
Release 8.6R1; Drop Eligible and Vlan-priority fields removed.

Related Commands

saa spb                Configures an SPB SAA.
saa spb reset          Resets SPB SAA parameters to their default values.
saa spb flush          Clears SPB SAA sessions and rebuilds the sessions based on learned SPB information.

MIB Objects

alaSaaSspbFeature
  alaSaaSspbAutoCreate
  alaSaaSspbAutoStart
  alaSaaSspbInterval
  alaSaaSspbVlanPriority
  alaSaaSspbDropEligible
  alaSaaSspbPktData
  alaSaaSspbNumPkts
  alaSaaSspbInterPktDelay
  alaSaaSspbPayloadSize
  alaSaaSspbJitterThreshold
  alaSaaSspbRTTThreshold
  alaSaaSspbKeep
show saa xml

Displays the SAA XML file generation parameter configuration.

show saa xml

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples
-> show saa xml

XML file creation parameters:
Admin status : Disabled,
File : saa.xml,
Interval : 20

output definitions
<table>
<thead>
<tr>
<th>Admin status</th>
<th>The status (Enabled or Disabled) of SAA XML history file generation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>The name of the XML file to which SAA writes session history entries.</td>
</tr>
<tr>
<td>Interval</td>
<td>The amount of time, in minutes, between each generation of the XML history file.</td>
</tr>
</tbody>
</table>

Release History
Release 7.3.2; command was introduced.
Related Commands

saa xml

Configures SAA XML file generation parameters.

MIB Objects

alaSaaXmlFeature
alaSaaXmlStatus
alaSaaXmlFilename
alaSaaXmlInterval
**show saa statistics**

Display SAA statistics.

```
[vrf vrf_name] show saa [string] statistics [aggregate | history]
```

---

**Syntax Definitions**

- **vrf_name**: The name of an existing VRF instance.
- **string**: An existing SAA ID string.
- **aggregate**: Displays aggregate results for the specified SAA.
- **history**: Displays a results history for the specified SAA.

---

**Defaults**

By default, statistics are displayed for all SAAs and only for the most recent SAA test run.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>V72/C32</th>
<th>X48C6/T48C6</th>
<th>X48C4E/V48C8</th>
<th>C32E/T24C2</th>
<th>X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- If the **aggregate** parameter is specified, then only the aggregate results are displayed.
- If the **history** parameter is specified, then only the history results are displayed.
- Since results are only kept for the last five iterations, using the **history** option displays only the last five iterations of each SAA test.
- Specify the SAA ID to display statistics for a specific SAA.
- Statistics and history do not persist across a switch reboot or takeover.

---

**Examples**

```
-> show saa statistics
Legend: eth-lb  = ethoam-loopback
        eth-dmm = ethoam-two-way-delay
        - = Delay or jitter value not available

Aggregate Record:
SAA  Owner  Type   Time of Last-Run    RTT  RTT  RTT  RTT   Jitter  Jitter  Jitter  Jitter  Packets
Description     Min  Avg  Max  Thr  Min  Avg  Max  Thr  Sent  Rcvd
-----------------------+----+----+----+----+----+----+----+----+----+----+
saa1 USER ip-ping 2013-06-19,12:52:52.0 970 1067 1432 -    1    99  455   -    7   7 DEFAULT
```
Service Assurance Agent Commands

```
saa2 USER ip-ping 2013-06-19,11:06:02.0 192 238 383 200 15 62 191 150 5 5 DEFAULT
saa3 USER eth-dmm 2013-06-19,12:52:25.0 1563 2664 3574 - - 15 27 173 - 5 5 DEFAULT
saa4 USER eth-lb 2013-06-19,22:30:40.0 1243 1537 2166 100 23 42 96 500 6 6 DEFAULT
```

-> show saa statistics history
Legend: eth-lb = ethoam-loopback
     eth-dmm = ethoam-two-way-delay
- - Delay or jitter value not available

History Records SAA: saa1

<table>
<thead>
<tr>
<th>Type</th>
<th>Time of Last-Run</th>
<th>RTT Min</th>
<th>RTT Avg</th>
<th>RTT Max</th>
<th>Jitter Min</th>
<th>Jitter Avg</th>
<th>Jitter Max</th>
<th>Jitter Thr</th>
<th>Packets Sent</th>
<th>Result</th>
<th>Descr</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-ping</td>
<td>2013-06-19,14:06:08.0</td>
<td>175</td>
<td>205</td>
<td>281</td>
<td>500</td>
<td>4</td>
<td>39</td>
<td>106</td>
<td>150</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>ip-ping</td>
<td>2013-06-19,14:04:26.0</td>
<td>171</td>
<td>209</td>
<td>307</td>
<td>500</td>
<td>11</td>
<td>51</td>
<td>125</td>
<td>150</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>ip-ping</td>
<td>2013-06-19,13:36:02.0</td>
<td>181</td>
<td>199</td>
<td>245</td>
<td>500</td>
<td>1</td>
<td>23</td>
<td>64</td>
<td>150</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>ip-ping</td>
<td>2013-06-19,11:06:02.0</td>
<td>192</td>
<td>238</td>
<td>383</td>
<td>500</td>
<td>15</td>
<td>62</td>
<td>191</td>
<td>150</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

```
-> show saa ip-ping statistics aggregate
SAA: ip-ping

Total numbers of iterations : 4
Aggregated Record:
- Total Packets Sent : 20,
- Total Packets Received : 20,
- Avg RTT-Min/Avg/Max (micro sec) : 171/212/383,
- Avg Jitter-Min/Avg/Max (micro sec) : 1/43/191,
- Timestamp-Min RTT : 2013-06-19,14:04:26.0,
- Timestamp-Max RTT : 2013-06-19,11:06:02.0,
- Timestamp-Min Jitter : 2013-06-19,13:36:02.0,
- Timestamp-Max Jitter : 2013-06-19,11:06:02.0
```

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAA</td>
<td>SAA name</td>
</tr>
<tr>
<td>Owner</td>
<td>The owner name assigned to the agent.</td>
</tr>
<tr>
<td>Type</td>
<td>The SAA type.</td>
</tr>
<tr>
<td>Time of Last Run</td>
<td>The time the SAA was last run.</td>
</tr>
<tr>
<td>RTT Min</td>
<td>The round trip minimum value.</td>
</tr>
<tr>
<td>RTT Avg</td>
<td>The round trip average value.</td>
</tr>
<tr>
<td>RTT Max</td>
<td>The round trip maximum value.</td>
</tr>
<tr>
<td>RTT Thr</td>
<td>The round-trip time threshold value, in microseconds.</td>
</tr>
<tr>
<td>Jitter Min</td>
<td>The jitter minimum value.</td>
</tr>
<tr>
<td>Jitter Avg</td>
<td>The jitter average value.</td>
</tr>
<tr>
<td>Jitter Max</td>
<td>The jitter maximum value.</td>
</tr>
<tr>
<td>Jitter Thr</td>
<td>The jitter threshold value, in microseconds.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Number of packets sent during all the ping iterations.</td>
</tr>
<tr>
<td>Packets Rcvd</td>
<td>Number of packets received during all the ping iterations.</td>
</tr>
<tr>
<td>Description</td>
<td>Configured description for the SAA.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.3.1; command was introduced.
Release 7.3.2: **Owner, RTT Thr**, and **Jitter Thr** fields added.
Related Commands

saa

Configures a SAA.

MIB Objects

alaSaaIpResultsTable

alaSaaIpResultsPktsSent
alaSaaIpResultsPktsRcvd
alaSaaIpResultsRunResultReason
alaSaaIpResultsRunTime
alaSaaIpResultsMinRTT
alaSaaIpResultsAvgRTT
alaSaaIpResultsMaxRTT
alaSaaIpResultsMinJitter
alaSaaIpResultsAvgJitter
alaSaaIpResultsMaxJitter

alaSaaEthoamResultsTable

alaSaaEthoamResultsPktsSent
alaSaaEthoamResultsPktsRcvd
alaSaaEthoamResultsRunResultReason
alaSaaEthoamResultsRunTime
alaSaaEthoamResultsMinRTT
alaSaaEthoamResultsAvgRTT
alaSaaEthoamResultsMaxRTT
alaSaaEthoamResultsMinJitter
alaSaaEthoamResultsAvgJitter
alaSaaEthoamResultsMaxJitter

alaSaaIpCtrlTable

alaSaaIpCtrlTotalPktsSent
alaSaaIpCtrlTotalPktsRcvd
alaSaaIpCtrlMinRTT
alaSaaIpCtrlAvgRTT
alaSaaIpCtrlMaxRTT
alaSaaIpCtrlMinJitter
alaSaaIpCtrlAvgJitter
alaSaaIpCtrlMaxJitter

alaSaaEthoamCtrlTable

alaSaaEthoamCtrlTotalPktsRcvd
alaSaaEthoamCtrlTotalPktsSent
alaSaaEthoamCtrlMinRTT
alaSaaEthoamCtrlAvgRTT
alaSaaEthoamCtrlMaxRTT
alaSaaEthoamCtrlMinJitter
alaSaaEthoamCtrlAvgJitter
alaSaaEthoamCtrlMaxJitter
show saa vrf

Display SAA statistics for the IP ping sessions.

show saa {vrf vrf_name | all} [statistics [aggregate | history]]

Syntax Definitions

vrf_name
   Displays the results for the specified SAA IP pings from a specific VRF.

all
   Displays the results for the SAA IP pings from all VRF across the system.

statistics
   Displays the statistics for the most recent SAA IP ping test run.

aggregate
   Displays aggregate results for the specified SAA IP ping.

history
   Displays a results history for the specified SAA IP ping.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the aggregate parameter is specified, then only the aggregate results are displayed.
- If the history parameter is specified, then only the history results are displayed.
- Since results are only kept for the last five iterations, using the history option displays only the last five iterations of each SAA test and in each SAA history, iteration information of first 20 received packets are stored.
- Statistics and history do not persist across a switch reboot or takeover.
- The show output will be filtered based on the corresponding VRF. Any VRF name that auto-completes to “all” will be taken as the keyword “all”, and all the IP ping sessions across the VRFs is displayed.

Examples

--> show saa vrf all
SAA Owner  Type   Status  Interval Time of Last Run Last Run Result Description  VRF Name
(min)                          ===================================================
ip100 USER ip-ping started 2 2020-01-26,22:45:46.0 success DEFAULT VRF1
ip200 USER ip-ping started 2 2020-01-26,22:45:35.0 success DEFAULT VRF2
Service Assurance Agent Commands

```
show saa vrf

-> show saa vrf BLUE
SAA  Owner  Type   Status  Interval Time of Last Run Last Run Result Description  VRF Name
----+-----+-------+-------+--------+----------------+---------------+-----------+----------
ip100 USER  ip-ping started     2       2020-01-26,22:45:46.0   success    DEFAULT    VRF1

-> show saa vrf all statistics
Legend: - = Delay or jitter value not available
Aggregate Record:
SAA Owner Type Time of Last-Run RTT RTT RTT RTT Jitter Jitter Jitter Jitter Packets Description VRFName
---+-----+---+-----------------+---+---+---+---+-----+-------+-------+-----+---------+----------+------
ip100 USER ip-ping 2020-01-26,22:45:46.0  1102 1431 2091 0 31  204   478    0    5    5 DEFAULT   VRF1
ip200 USER ip-ping 2020-01-26,22:45:35.0  1035 3331 12469 0 5  2290  11415  0    5    5 DEFAULT   VRF2
```

**output definitions**

<table>
<thead>
<tr>
<th>SAA</th>
<th>SAA name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>The owner name assigned to the agent.</td>
</tr>
<tr>
<td>Type</td>
<td>The SAA type.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the SAA test: started or stopped.</td>
</tr>
<tr>
<td>Interval (min)</td>
<td>Interval of the SAA.</td>
</tr>
<tr>
<td>Time of Last Run</td>
<td>The time the SAA was last run.</td>
</tr>
<tr>
<td>Last Run Result</td>
<td>Result of last iteration.</td>
</tr>
<tr>
<td>Description</td>
<td>Configured description for the SAA.</td>
</tr>
<tr>
<td>VRF Name</td>
<td>Name of the VRF.</td>
</tr>
<tr>
<td>RTT Min</td>
<td>The round trip minimum value.</td>
</tr>
<tr>
<td>RTT Avg</td>
<td>The round trip average value.</td>
</tr>
<tr>
<td>RTT Max</td>
<td>The round trip maximum value.</td>
</tr>
<tr>
<td>RTT Thr</td>
<td>The round-trip time threshold value, in microseconds.</td>
</tr>
<tr>
<td>Jitter Min</td>
<td>The jitter minimum value.</td>
</tr>
<tr>
<td>Jitter Avg</td>
<td>The jitter average value.</td>
</tr>
<tr>
<td>Jitter Max</td>
<td>The jitter maximum value.</td>
</tr>
<tr>
<td>Jitter Thr</td>
<td>The jitter threshold value, in microseconds.</td>
</tr>
<tr>
<td>Packets Sent</td>
<td>Number of packets sent during all the ping iterations.</td>
</tr>
<tr>
<td>Packets Rcvd</td>
<td>Number of packets received during all the ping iterations.</td>
</tr>
<tr>
<td>Description</td>
<td>Configured description for the SAA.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.7R1: command introduced.
Related Commands

\textbf{saa} \hspace{2cm} Configures a SAA.

\textbf{MIB Objects}

alaSaaIpResultsTable
  \textbf{alaSaaIpResultsPktsSent}
  \textbf{alaSaaIpResultsPktsRcvd}
  \textbf{alaSaaIpResultsRunResultReason}
  \textbf{alaSaaIpResultsRunTime}
  \textbf{alaSaaIpResultsMinRTT}
  \textbf{alaSaaIpResultsAvgRTT}
  \textbf{alaSaaIpResultsMaxRTT}
  \textbf{alaSaaIpResultsMinJitter}
  \textbf{alaSaaIpResultsAvgJitter}
  \textbf{alaSaaIpResultsMaxJitter}

alaSaaIpCtrlTable
  \textbf{alaSaaIpCtrlTotalPktsSent}
  \textbf{alaSaaIpCtrlTotalPktsRcvd}
  \textbf{alaSaaIpCtrlMinRTT}
  \textbf{alaSaaIpCtrlAvgRTT}
  \textbf{alaSaaIpCtrlMaxRTT}
  \textbf{alaSaaIpCtrlMinJitter}
  \textbf{alaSaaIpCtrlAvgJitter}
  \textbf{alaSaaIpCtrlMaxJitter}
The Chassis Management Module (CMM) CLI commands permit you to manage switch software files on the CMM.

MIB information for the CMM commands is as follows:

- **Filename**: ALCATEL-IND1-CHASSIS-MIB.mib
  - **Module**: alcatelIND1ChassisMIB

- **Filename**: ALCATEL-IND1-CONFIG-MGR-MIB DEFINITIONS.mib
  - **Module**: alcatelIND1ConfigMgrMIB

A summary of available commands is listed here:

```
reload secondary
reload slot
reload all
reload from
issu from
issu slot
write memory
reload chassis-id
copy certified
copy running certified
modify running-directory
copy flash-synchro
takeover
show running-directory
show reload
show microcode
show issu status
usb
usb backup admin-state
usb auto-copy
mount
umount
show usb statistics
auto-config-abort
image integrity check
image integrity get-key
```
reload secondary

Reloads the secondary CMM from the **certified** directory.

```
reload [chassis-id \textit{chassis}] secondary \textit{in [hours:] minutes | at hour:minute [month day | day month]}
```

```
reload secondary cancel
```

### Syntax Definitions

- **chassis**: The chassis identifier.
- **in \textit{[hours:] minutes}**: Optional syntax. Schedules a reload of the software to take effect in the time. The time can be specified in minutes or hours and minutes within the next 24 hours.
- **at \textit{hour:minute}**: Optional syntax. Schedules a reload of the software to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
- **month day | day month**: The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. See examples below for further explanation.
- **cancel**: Cancels a pending time delayed reboot.

### Defaults

N/A

### Platforms Supported

Not supported in this release.

### Usage Guidelines

- Can be issued from both primary or secondary CMM.
- Reloads the secondary CMM only, the Primary CMM remains operational.

### Examples

```
-> reload secondary
-> reload secondary in 15:25
-> reload secondary at 15:25 august 10
-> reload secondary at 15:25 10 august
```

### Release History

Release 7.1.1; command introduced.
Related Commands

reload from

Reloads both CMMs from the specified directory.

MIB Objects

chasEntPhysicalTable
  csEntPhysicalIndex
  chasEntPhysAdminStatus
chasControlRedundantTable
  chasControlDelayedRebootTimer
**reload all**

Reloads both Chassis Management Modules (CMMs) from the *certified* directory.

```
reload [chassis-id chassis] all [in [hours:] minutes | at hour:minute [month day | day month]]
```

**reload all cancel**

**Syntax Definitions**

- `chassis` The chassis identifier.
- `in [hours:] minutes` Optional syntax. Schedules a reload of all modules to take effect in the specified minutes or hours and minutes within the next 24 hours.
- `at hour:minute` Optional syntax. Schedules a reload of all modules to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
- `month day | day month` The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. It is unimportant if the month or day is first. See examples below for further explanation.
- `cancel` Cancels a pending time delayed reload.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Can be issued from the Primary CMM only.

**Examples**

- `-> reload all`
- `-> reload all in 1:30`
- `-> reload all at 12:00 july 25`
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

*reload slot*  
Reloads a specific NI module.

**MIB Objects**

chasEntPhysicalTable
  chasEntPhysAdminStatus
chasGlobalControl
  chasGlobalControlDelayedResetAll
reload from

Reloads both CMMs from the specified directory. There is no CMM failover during this reboot, causing a loss of switch functionality during the reboot. All the NIs and the secondary CMM will reload.

```
reload [chassis-id chassis] from image_dir {rollback-timeout minutes | no rollback-timeout [in [hours:] minutes | at hour:minute] [redundancy-time minutes]}
```

### Syntax Definitions

- **chassis**
  The chassis identifier when running in virtual chassis mode.
- **image_dir**
  The directory that contains the image files to be loaded onto the switch.
- **rollback-timeout minutes**
  Sets a timeout period, in minutes. The switch immediately reboots from the specified directory. At the end of this time period, the switch automatically reboots again from the **certified** directory. The valid range of rollback timeout minutes is 1–15.
- **no rollback-timeout**
  Specifies no timeout to rollback. If the command is issued with this keyword, then the switch continues to run from the specified directory until manually rebooted.
- **in [hours:] minutes**
  Optional syntax. Schedules a reload of the to take effect in the specified minutes or hours and minutes within the next 24 hours.
- **at hour:minute**
  Optional syntax. Schedules a reload to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
- **redundancy-time minutes**
  Specifies the time period in minutes that the switch must run without failure. If a failure occurs within this time period, the switch will reboot from the **certified** directory.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Can be issued from Primary CMM only.
- This command is used to reload the switch from the specified directory.

- A file verification will be performed before rebooting to ensure all necessary files are present and valid. An error message will be displayed describing any issues found.

- The image directory reload takes place immediately unless a time frame is set using the `in` or `at` keywords.

- If a rollback-timeout is set, the switch reboots again after the set number of minutes, from the `certified` directory. The reboot can be halted by issuing a cancel order as described in the `reload all` command.

- If the `redundancy-time` parameter is entered, any reboot of the Primary CMM prior to the redundancy timer expiring will cause the switch to reboot. If the Primary CMM reboots after the redundancy timer expires, the secondary CMM will take over without a reboot.

**Examples**

- `reload from working rollback-timeout 5`
- `reload from working no rollback-timeout`
- `reload from working no rollback-timeout in 50`
- `reload from working rollback-timeout 10 at 12:50`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `reload all` Reboots both CMMs from the `certified` directory.

**MIB Objects**

- `chasControlModuleTable`
  - `chasControl`
  - `chasControlVersionMngt`
  - `chasControlActivateTimeout`
  - `chasControlRedundancyTime`
  - `chasControlDelayedActivateTimer`
  - `chasControlWorkingVersion`
  - `chasControlNextRunningVersion`
**reload slot**

Reloads the NI in the specified slot using the current running image.

```
reload slot chassis/slot
```

---

### Syntax Definitions

- **chassis**: The chassis identifier.
- **slot**: The slot number to be reloaded.

### Defaults

N/A

### Platforms Supported

Not supported in this release.

### Usage Guidelines

Can be issued from Primary CMM only.

### Examples

```
-> reload slot 1/2
```

### Release History

Release 7.1.1; command introduced.

### Related Commands

- **reload from**: Reloads both CMMs from the specified directory.

### MIB Objects

- `chasEntPhysicalTable`
  - `chasEntPhysAdminStatus`

---
**reload chassis-id**

Reloads the specified chassis id when running in virtual chassis mode.

```
reload chassis-id chassis [all] [in [hours:] minutes | at hour:minute [month day | day month]]
```

```
reload chassis-id cancel
```

---

**Syntax Definitions**

- `chassis` The chassis identifier.
- `in [hours:] minutes` Optional syntax. Schedules a reload of the software to take effect in the time. The time can be specified in minutes or hours and minutes within the next 24 hours.
- `at hour:minute` Optional syntax. Schedules a reload of the software to take place at the specified time using a 24-hour clock. If you do not specify the month and day, the reload takes place at the specified time on the current day provided the specified time is later than the time when the CLI command is issued. If the specified time is earlier than the current time, the reload takes place on the following day.
- `month day | day month` The name of the month and the number of the day for the scheduled reload. Specify a month name and the day number. See examples below for further explanation.
- `cancel` Cancels a pending time delayed reboot.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Yes</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Can be issued from both primary or secondary CMM.
- Reloads the secondary CMM only, the Primary CMM remains operational.

---

**Examples**

```
-> reload chassis-id 1
-> reload chassis-id 1 in 15:25
-> reload chassis-id 1 at 15:25 august 10
```
- reload chassis-id 1 at 15:25 10 august
- reload chassis-id 1 cancel

**Release History**
Release 7.3.1; command introduced.

**Related Commands**
- **reload from**
  Reloads both CMMs from the specified directory.

**MIB Objects**
- `chasEntPhysicalTable`
- `csEntPhysicalIndex`
- `chasEntPhysAdminStatus`
- `chasControlRedundantTable`
- `chasControlDelayedRebootTimer`
copy certified

Copies the contents of the certified directory to the specified directory.

```
copy certified image_dir [make-running-directory]
```

**Syntax Definitions**

- `image_dir` - The directory that the contents of the certified directory will be copied to.
- `make-running-directory` - Makes the destination directory the new RUNNING DIRECTORY after the configuration is copied.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Using the `make-running-directory` parameter changes the RUNNING DIRECTORY allowing changes to be saved using the `write memory` command.
- This command does not delete any extra files in the target directory.
- This command does not affect the synchronization status of the running configuration.
- To synchronize the running and saved configuration, use the `write memory` command.

**Examples**

```
-> copy certified mydir
-> copy certified mydir make-running-directory
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

**copy flash-synchro**  
Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

chasControlModuleTable
- chasControlVersionMngt
- chasControlWorkingVersion
### issu from

Upgrades the system with the images stored in the specified directory with minimal disruption to traffic.

`issu from image_dir [redundancy-time minutes]`

<table>
<thead>
<tr>
<th>Syntax Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>image_dir</code></td>
</tr>
<tr>
<td><code>redundancy-time minutes</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The new code must support ISSU with the current running version of code.
- A text file named ‘`issu_version`’ is used to determine ISSU compatibility between code versions. It can be downloaded from the Service and Support website and must be included in the directory along with the new image files.

**Examples**

`-> issu from myissu`

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- `issu slot` Causes a power-cycle of the NI in the specified slot after an ISSU upgrade.

**MIB Objects**

- `chasEntModuleTable`
chasControlWorkingVersion
chasControlRedundancyTime
**issu slot**

Causes a reset of the NI in the specified slot after an ISSU upgrade.

```
issu slot num
```

**Syntax Definitions**

`num` Specifies the slot number.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Will return an error if ISSU is not in progress or if the slot has already been reset after the ISSU.

**Examples**

```
-> issu slot 2
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`issu from` Upgrades the system with the images stored in the specified directory without disruption to traffic.

**MIB Objects**

chasEntPhysicalTable

entPhysicalIndex
**write memory**

Copies the current configuration (RAM) to the RUNNING DIRECTORY on the primary CMM.

`write memory [flash-synchro]`

---

**Syntax Definitions**

`flash-synchro`  
Synchronizes the primary and secondary CMM.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- This command is used to copy the changes performed using the CLI commands from the running configuration (RAM) to the RUNNING DIRECTORY.

- The `flash-synchro` keyword synchronizes the files between the primary and secondary CMMs by overwriting the contents of the secondary CMM **certified** directory with the contents of the primary CMM certified directory.

- This command is only valid if the switch isn’t running from the **certified** directory. Use the `show running-directory` command to check where the switch is running from.

- During flash synchronization configuration changes may time out causing error messages to be displayed. Once the synchronization is complete configuration changes can resume.

---

**Examples**

- `-> write memory`
- `-> write memory flash-synchro`

---

**Release History**

Release 7.1.1; command introduced.
Related Commands

**copy flash-synchro**

Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

```plaintext
configManager
  configWriteMemory
```
copy running certified

Copies the current RUNNING DIRECTORY configuration to the certified directory on both CMMs.

`copy running certified [flash-synchro]`

---

**Syntax Definitions**

| flash-synchro | Synchronizes the primary and secondary CMM. |

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

| 6360 | 6465 | 6560 | 6570M | 6860 | 6860N | 6865 | 6900 | 6900
| Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

**Usage Guidelines**

- This command is used to overwrite the contents of the certified directory with the configuration from the RUNNING DIRECTORY. This should only be done if the running configuration has been verified.
- This command only synchronizes the image and configuration files in the RUNNING DIRECTORY, no other directories, such as the switch or network directories, are synchronized.
- The flash-synchro keyword synchronizes the files between the primary and secondary CMMs by overwriting the contents of the secondary CMM certified directory with the contents of the primary CMM certified directory. Beginning in 7.3.1 the flash-synchro functionality is done automatically; entering the flash-synchro parameter is no longer required.
- In 7.3.3 the flash-synchro parameter will display an error on the OS6900 if there is no secondary CMM.
- If there is not enough free space, the copy attempt fails and an error message is generated.
- This command does not work if the switch is running from the certified directory. To view where the switch is running from, see the show running-directory command.
- This command may take up to two minutes to complete.

**Examples**

`-> copy running certified`
Release History

Release 7.1.1; command introduced.
Release 7.3.1; flash-synchro parameter no affect; the functionality is performed automatically.

Related Commands

copy flash-synchro
Copies the startup primary flash version of the CMM software to the startup secondary flash version of the CMM software.

MIB Objects

chasControlModuleTable
chasControlVersionMngt
chasControlWorkingVersion
modify running-directory

Changes the RUNNING DIRECTORY to the specified directory.

modify running-directory image_dir

Syntax Definitions

image_dir The directory name to become the new RUNNING DIRECTORY.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to change the RUNNING DIRECTORY and allow configuration changes to be saved to the new RUNNING DIRECTORY.

Examples

-> modify running-directory user-config1
-> write memory

Release History

Release 7.1.1; command introduced.

Related Commands

write memory Copies the running primary RAM version of the CMM software to the RUNNING DIRECTORY.

MIB Objects

chasControlModuleTable
   CurrentRunningVersion
copy flash-synchro

Copies the certified directory version of the primary CMM software to the certified directory of the secondary CMM.

copy flash-synchro

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
Not supported in this release.

Usage Guidelines

- This command is used to synchronize the certified directories of the primary and secondary CMMs. The two CMMs must be synchronized if a fail over occurs, otherwise switch performance is affected.

- This command is a shorter version of the ‘copy running certified flash-synchro’ command. Beginning in 7.3.1 the flash-synchro functionality is done automatically; this command is no longer required.

Examples
-> copy flash-synchro
-> configure copy flash-synchro

Release History
Release 7.1.1; command introduced.

Related Commands

copy running certified

Copies the RUNNING DIRECTORY configuration to the certified directory on the primary CMM.

MIB Objects
chasControlModuleTable
chasControlVersionMngt
**takeover**

Forces the current secondary CMM to assume the role of the primary CMM.

```
takeover [chassis]
```

---

**Syntax Definitions**

- `chassis`: The chassis identifier.

---

**Defaults**

N/A

---

**Platforms Supported**

Not supported in this release.

---

**Usage Guidelines**

- This command causes the secondary CMM to take over the functions of the primary CMM. After this command, the old primary CMM is the new secondary CMM.

- Be sure that the secondary CMM has all software (i.e., image and configuration files) required to continue CMM operations, before issuing the `takeover` command.

- For information on synchronizing the primary and secondary CMM software before issuing the `takeover` command, see the `copy flash-synchro` command.

---

**Examples**

```
-> takeover
```

---

**Release History**

Release 7.1.1; command introduced.

---

**Related Command**

- `reload all`: Reboots the switch.

---

**MIB Objects**

- `chasEntPhysicalTable`
  - `chasEntPhysAdminStatus`
show running-directory

Shows the current state of version and configuration management for a CMM.

show running-directory

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Once a switch boots up and is running, it runs either from the *working*, *certified*, or a *user-defined* directory. If the switch is running from the *certified* directory, changes made to the RUNNING CONFIGURATION using CLI commands, cannot be saved.

- Depending on the switch configuration there may be a small delay before the information is displayed.

Examples

-> show running-directory

CONFIGURATION STATUS
  Running CMM : PRIMARY,
  CMM Mode : MONO CMM,
  Current CMM Slot : A,
  Running configuration : CERTIFIED,
  Certify/Restore Status : CERTIFIED,

SYNCHRONIZATION STATUS
  Flash Between CMMs : SYNCHRONIZED
  Running Configuration : SYNCHRONIZED

BOOT STATUS
  Machine State : SHUTDOWN

output definitions

Running CMM The CMM currently controlling the switch, either PRIMARY or SECONDARY.

CMM Mode Whether there are one or two CMMs installed or Virtual Chassis mode.
**output definitions (continued)**

<table>
<thead>
<tr>
<th>Description</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current CMM Slot</td>
<td>The slot of the primary CMM, A or B.</td>
</tr>
<tr>
<td>Running Configuration</td>
<td>The current RUNNING DIRECTORY.</td>
</tr>
<tr>
<td>Certify/Restore Status</td>
<td>Indicates if the CMM has been certified.</td>
</tr>
<tr>
<td>Flash Between CMMs</td>
<td>SYNONCHRONIZED: Flash between CMMs is identical.</td>
</tr>
<tr>
<td></td>
<td>NOT SYNCHRONIZED: Flash between CMMs is not identical.</td>
</tr>
<tr>
<td>Running Configuration</td>
<td>SYNONCHRONIZED: RUNNING CONFIGURATION has been saved to the RUNNING DIRECTORY.</td>
</tr>
<tr>
<td></td>
<td>NOT SYNCHRONIZED: RUNNING CONFIGURATION has not been saved to the RUNNING DIRECTORY.</td>
</tr>
<tr>
<td>Machine State</td>
<td>SHUTDOWN - When in VC mode, this indicates the chassis has shutdown due to the ‘virtual-chassis shutdown’ command or when the chassis has shutdown due to a VC error. It is only displayed if the chassis is in the shutdown state.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **reload all** Reboots the switch.
- **copy flash-synchro** Copies the *certified* directory version of the primary CMM software to the *certified* directory of the secondary CMM.

**MIB Objects**

- `chasControlModuleTable`
  - `chasControlSynchronizationStatus`
  - `chasControlCertifyStatus`
  - `chasControlRunningVersion`
- `chasEntPhysicalTable`
  - `chasEntPhysOperStatus`
  - `entPhysicalIndex`
- `chasControlReloadTable`
  - `chasControlReloadStatus`
show reload

Shows the status of any time delayed reboot(s) that are pending on the switch.

show reload [[chassis-id chassis] [status | all status]]

Syntax Definitions

chassis
The chassis identifier.

status
Displays whether or not either of the CMMs are scheduled for a reload.

all status
Displays whether or all the modules are scheduled for a reload.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>V72/C32</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• It is possible to preset a reboot on a CMM by using the reload command. If this is done, use the show reload command to see when the next scheduled reboot is going to occur.

• If the reload from command is used, and a rollback timeout is set, the rollback occurs and is shown using the show reload command.

Examples

-> show reload status
Primary Control Module Reload Status: No Reboot Scheduled,
Secondary Control Module Reload Status: No Reboot Scheduled

Release History

Release 7.1.1; command introduced.
Related Commands

reload secondary  Reboots the primary or secondary CMM to its startup software configuration.
reload from  Immediate primary CMM reboot to the specified software configuration without secondary CMM takeover.

MIB Objects

chasControlModuleTable
   chasControlDelayedActivateTimer
chasGlobalControl
   chasGlobalControlDelayedResetAll
**show microcode**

Displays microcode versions installed on the switch.

```
show microcode [working | certified | loaded | issu | image_dir]
```

### Syntax Definitions
- **working**: Specifies the `working` directory.
- **certified**: The chassis identifier when running in virtual chassis mode.
- **loaded**: Specifies the loaded (i.e., currently-active) microcode versions.
- **issu**: Specifies the `issu` directory.
- **image_dir**: Specifies the user-defined directory.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>microcode</td>
<td>loaded</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If no additional parameters are entered the command defaults to the `loaded` parameter and the currently active microcode information is displayed.

- If a different version of code than the currently active version is copied to the RUNNING directory the image will be marked as ‘Stale’.

### Examples

```
-> show microcode
Package           Release       Size     Description
-----------------+---------------+--------+-----------------------------------
Ros.img           7.1.1.403.R01    1828255 Alcatel-Lucent OS
Renl.img      7.1.1.403.R01    1359435 Alcatel-Lucent NI
```
**output definitions**

<table>
<thead>
<tr>
<th>Package</th>
<th>File name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Version number.</td>
</tr>
<tr>
<td>Size</td>
<td>File size.</td>
</tr>
<tr>
<td>Description</td>
<td>File description.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

*usb*  
Displays the archive history for microcode versions installed on the switch.

**MIB Objects**

* N/A
usb

Enables access to the device connected to the USB port.

*usb {enable | disable}*

**Syntax Definitions**

N/A

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If an Alcatel-Lucent Enterprise certified USB device is connected after enabling the USB interface, the device will be automatically mounted as `/uflash`.
- Once mounted, common file and directory commands can be used for file management.

**Examples**

- `usb enable`
- `cp /flash/working/boot.cfg /uflash/boot.cfg`
- `ls /uflash`

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**usb auto-copy**
Allows backup image files from the USB device to be automatically copied to the /flash/working directory on the switch immediately after the USB device is connected.

**usb backup admin-state**
Enables or disables USB backup on the switch.

MIB Objects

```plaintext
systemServices
  systemServicesUsbEnable
```
usb backup admin-state

Enables or disables USB backup on the switch.

```
usb backup admin-state {enable | disable} {[key string] | hash-key string [bootable]}
```

**Syntax Definitions**

- **enable**
  Enables Administrative control to USB backup on the switch.

- **disable**
  Disables Administrative control to USB backup on the switch.

- **key**
  Keyword which will be used for encryption. *This parameter is only supported on the OmniSwitch 6465.*

- **hash-key**
  Keyword which will be decrypted and then used for encryption. *This parameter is only supported on the OmniSwitch 6465.*

- **bootable**
  Keyword which will enable the advanced backup. *This parameter is only supported on the OmniSwitch 6465 and OmniSwitch 6865.*

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When this command is enabled, the images and configuration from certified and running directories are copied into /uflash/6860/certified and /uflash/6860/running directories.

- When `write memory` is executed and backup is enabled, the configuration files from /flash/running-directory are copied to /uflash/6860/running-directory name.

- When `usb backup admin-state` is enabled and `copy running certified` and `write memory flash-synchr` commands are executed, the configuration and images from /flash/certified will be copied to /uflash/6860/certified.

- If the image files are manually deleted from /uflash after a backup subsequent `write memory flash-synchr` commands will not copy the image files /uflash again. Use the `usb backup` command to disable and re-enable usb backup and copy the image files to /uflash again.
• Encryption is supported only on the OmniSwitch 6465.
  – When a key or hash key is specified, all of the configuration files and images will be encrypted and copied to the USB device.
  – If a key or hash key is not specified, all of the configuration files and images will be copied as is to the USB device.
  – Maximum length of key should be 32 characters. Minimum key length should be 8 characters.
  – If the user has gone through one back up cycle of encryption and wants to disable encryption, then the user must disable the USB back up and enable it again with no password.
• On the OmniSwitch 6465, when power supply configurations are added by the powersupply enable command, the power supply configurations are backed up in /uflash/6465/system folder when backup is enabled.
• Back-up cannot be enabled if auto-copy is enabled and auto-copy cannot be enabled if back-up is enabled. So only one of these features can be enabled at any given time.
• The bootable option is used to indicate advanced backup. The advanced backup is supported only on OmniSwitch 6465 and OmniSwitch 6865 platforms.
• When bootable option is enabled:-
  – The images from certified and running directories are copied into /uflash/6465/certified and /uflash/6465/running directories as the existing USB backup.
  – Compress the files (along with directory path) and use it for switch operation located in /flash to a tar file, then encrypt it with input key / hash-key as “configuration.tar.enc” and copy the output file to /uflash/6465 directory.

Examples

-> usb backup admin-state enable
-> usb backup admin-state disable
-> usb backup admin-state enable key “abc12345”
-> usb backup admin-state enable hash-key “a05234d”
-> usb backup admin-state enable key “abc12345” bootable
-> usb backup admin-state enable hash-key “a05234d” bootable

Release History

Release 8.5R1; command was introduced.
Release 8.5R2; key and hash-key parameter added.
Release 8.8R1; bootable parameter added.

Related Commands

usb auto-copy
  Allows backup image files from the USB device to be automatically copied to the /flash/working directory on the switch immediately after the USB device is connected

usb
  Enables access to the device connected to the USB interface.

show usb statistics
  Displays the status USB setting and features.

MIB Objects

systemServices
  systemServicesUsbBackupAdminState
systemServicesUsbBackupKey
systemServicesUsbBackupHashkey
systemServicesUsbBackupBootable
**usb auto-copy**

Allows the image files from the USB device to be automatically copied to the switch immediately after the USB device is connected.

```
usb auto-copy {enable | disable} copy-config {enable| disable} [key string | hash-key string ]
```

**Syntax Definitions**

- `enable`: Enables Administrative control to USB auto copy on the switch
- `disable`: Disables Administrative control to USB auto copy on the switch
- `key`: Keyword which will be used for encryption. *This parameter is only supported on the OmniSwitch 6465.*
- `hash-key`: Keyword which will be decrypted and then used for encryption. *This parameter is only supported on the OmniSwitch 6465.*

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the automatic copy is successful the switch will automatically reboot.
- The USB device must contain the proper file structure and image files mentioned below and the USB root directory must contain a signature file named `aossignature`. The `aossignature` file can be a blank text file transferred to the switch.
- This operation will enable all of the image files from the `/uflash/6465/working` or `/uflash/6860/working` directory to be copied to the `/flash/working` directory.
- If the auto-copy is successful, the auto-copy feature will be disabled before rebooting the switch and must be re-enabled by the administrator for the next auto-copy process to execute. This will prevent running the same auto-copy multiple times.
- If `copy-config` is enabled, configuration files will also be copied in addition to image files to the `/flash/working` directory from `/uflash/6860/working` directory.
Encryption is supported only on the OmniSwitch 6465.
- When a key or hash key is specified, all of the configuration files and images will be decrypted and copied to the AOS flash.
- If a key or hash key is not specified, all of the configuration files and images will be copied as is to the AOS flash.
- Maximum length of key should be 32 characters. Minimum key length should be 8 characters.

On the OmniSwitch 6465, when power supply configurations are added by the `powersupply enable` command, the power supply configurations are backed up in `/uflash/6465/system` folder when backup is enabled.

Back-up cannot be enabled if auto-copy is enabled and auto-copy cannot be enabled if back-up is enabled. So only one of these features can be enabled at any given time.

**Examples**

```
-> usb auto-copy enable copy-config enable
-> usb auto-copy enable copy-config disable
-> usb auto-copy enable copy-config enable key "abc12345"
-> usb auto-copy enable copy-config enable hash-key "a05234d"
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R1; `copy-config` parameter added.
Release 8.5R2; `key` and `hash-key` parameter added.

**Related Commands**

- `usb backup admin-state` Enables or disables USB backup on the switch.

**MIB Objects**

- `systemServices` Enables access to the device connected to the USB interface.
  - `systemServicesUsbCopyConfig`
  - `systemServicesUsbBackupKey`
  - `systemServicesUsbBackupHashkey`
mount

Mounts a USB device on /uflash.

`mount [/uflash]`

---

**Syntax Definitions**

- `/uflash` The name of the file-system to mount.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Once the USB device is mounted most file and directory commands associated with the `/flash` file system can be used with `/uflash` such as: mkdir, rmdir, cd, rm, cp, ls.

---

**Examples**

- `-> mount /uflash`
- `-> ls /uflash`

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `umount` Unmounts the /uflash file system from AOS.

---

**MIB Objects**

- `systemServicesAction`
- `systemServicesArg1`
umount

Unmounts the /uflash file system from AOS.

`umount /uflash`

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command unmounts the USB drive and should be used prior to unplugging the USB drive to prevent possible data corruption.

**Examples**

`-> umount /uflash`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `mount` - Mounts the /uflash file system from AOS.

**MIB Objects**

- `systemServicesAction`
- `systemServicesArg1`
show usb statistics

Displays the status USB setting and features.

show usb statistics

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show usb statistics
Host scsi1: usb-storage
Vendor: USB3.0
Product: FLASH DRIVE
Serial Number: 0xxxxxxxxxxxxxxxx
Protocol: Transparent SCSI
Transport: Bulk
usb: enabled
usb auto-copy: disable
auto-copy in progress: No
usb mount mode: sync
usb backup: disable
usb auto-copy config-copy: disable
usb encryption: enable
usb bootable: enable

output definitions

<table>
<thead>
<tr>
<th>Definition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>usb</td>
<td>Status of USB device interface.</td>
</tr>
<tr>
<td>usb auto-copy</td>
<td>Status of USB auto-copy feature.</td>
</tr>
<tr>
<td>auto-copy in progress</td>
<td>Is the switch currently in the process of performing an auto-upgrade.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.
Release 8.8R1; `bootable` parameter added.

**Related Commands**

- `usb` Enables access to the device connected to the USB interface.
- `usb auto-copy` Allows backup files from the USB device to be automatically copied to the switch immediately after the USB device is connected.
- `mount` Mounts the `/uflash` file system.

**MIB Objects**

`systemServices`

- `systemServicesUsbEnable`
- `systemServicesUsbAutoCopyEnable`
- `systemServicesUsbDisasterRecoveryEnable`
show issu status

Displays the status of ISSU.

show issu status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show issu status
Slot    ISSU-Status
--------+-----------------+
1       ISSU Pending
2       ISSU Pending
3       ISSU Pending

-> show issu status
Slot    ISSU-Status
--------+-----------------+
1       ISSU Complete
2       ISSU Complete
3       ISSU Complete

output definitions

<table>
<thead>
<tr>
<th>Slot</th>
<th>Specifies the slot number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISSU-Status</td>
<td>Indicates the ISSU status for a slot: Pending - Slot has not been reset; upgrade is not complete. Complete - Slot has been reset; upgrade is complete.</td>
</tr>
</tbody>
</table>
**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>issu from</td>
<td>Upgrades the system with the images stored in the specified directory without disruption to traffic.</td>
</tr>
</tbody>
</table>

**MIB Objects**

N/A
auto-config-abort

Aborts the Automatic Remote Configuration download process.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to stop the Automatic Remote Configuration download process.

Examples

-> auto-config-abort

Release History

Release 7.3.4; command was introduced.

Related Commands

N/A

MIB Objects

N/A
image integrity check

Verifies whether the SHA256 hash key of an image file located in the specified directory matches the SHA256 hash key in the specified key file.

image integrity check image_dir key-file filename

Syntax Definitions

image_dir
The directory on the switch that contains the image file to verify. Enter the name of the directory in “/flash” or include the full path (for example, “working” or “/flash/working”).

filename
The name of the file that contains the key for the image file in the specified directory. Enter the name of the key file or include the full path (for example, “hash.txt” or “/flash/hash.txt”).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the name of the key file is specified without the directory path, the switch will look for the key file in the same directory specified for the image file.

- The following format is used to store the hash key values in the key file:
  Uos.img:f0ff173eff38e43e0598663da2185a363fcba5bd407201d7537d0a6b9f58670e

Example

-> image integrity check /flash/working key-file /flash/hash.txt
This operation may take several minutes...

Success: Key matched.

Release History

Release 8.3.1; command introduced.
Related Commands

**image integrity get-key**

Calculates and displays the SHA256 key for image files.

MIB Objects

- **systemServicesAction**
- **systemServicesArg1**
- **systemServicesArg2**
image integrity get-key

Displays the SHA256 hash key of the image present in the specified location.

image integrity get-key image_dir

Syntax Definitions

image_dir

The directory on the switch that contains the image file. Enter the name of the directory in “/flash” or include the full path (for example, “working” or “/flash/working”).

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When this command is entered, the SHA256 hash of the image files in the specified directory is calculated and displayed. It can be manually verified against the hash provided in the file.

- To store the hash key value in a text file that can be used with the image file integrity check command, use the following format:
  Uos.img:f0ff173eff38e43e0598663da2185a363fcba5bd407201d7537d0a6b9f58670e

Example

-> image integrity get-key /working
This operation may take several minutes...

<table>
<thead>
<tr>
<th>Image Name</th>
<th>SHA256 Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uos.img</td>
<td>c64d6b23312a6f9c4b99642b31ed087e600bce58d6fdd089d09e1f8077bd208</td>
</tr>
</tbody>
</table>

-> image integrity get-key /flash/certified
This operation may take several minutes...

<table>
<thead>
<tr>
<th>Image Name</th>
<th>SHA256 Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uos.img</td>
<td>3d4d488a73eb798325bac85793ef0d67bdf377527278a6732270d3a4801bb44b</td>
</tr>
</tbody>
</table>
**Release History**

Release 8.3.1; command introduced.

**Related Commands**

- **image integrity check**
  Verifies the SHA256 hash key for the image file matches the key specified in a text file.

**MIB Objects**

- systemServicesAction
- systemServicesArg1
- systemServicesArg2
Chassis Management and Monitoring commands allow you to configure and view hardware-related operations on the switch. Topics include basic system information, as well as Network Interface (NI) module and chassis management.

**Additional Information.** Refer to your separate *Hardware Users Guide* for detailed information on chassis components, as well as managing and monitoring hardware-related functions.

MIB information for the Chassis Management and Monitoring commands is as follows:

- **Filename:** ALCATEL-IND1-CHASSIS-MIB.mib  
  **Module:** alcatelIND1ChassisMIB

- **Filename:** ALCATEL-IND1-SYSTEM-MIB.mib  
  **Module:** alcatelIND1SystemMIB

- **Filename:** ALCATEL-IND1-CAPMAN-MIB.mib  
  **Module:** alcatelIND1CapManMIB
A summary of available commands is listed here:

<table>
<thead>
<tr>
<th>Management Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>system contact</td>
<td></td>
</tr>
<tr>
<td>system name</td>
<td></td>
</tr>
<tr>
<td>system location</td>
<td></td>
</tr>
<tr>
<td>system date</td>
<td></td>
</tr>
<tr>
<td>system time</td>
<td></td>
</tr>
<tr>
<td>system timezone</td>
<td></td>
</tr>
<tr>
<td>system daylight-savings-time</td>
<td></td>
</tr>
<tr>
<td>update uboot</td>
<td></td>
</tr>
<tr>
<td>update fpga-cpld</td>
<td></td>
</tr>
<tr>
<td>reload slot</td>
<td></td>
</tr>
<tr>
<td>power slot</td>
<td></td>
</tr>
<tr>
<td>powersupply enable</td>
<td></td>
</tr>
<tr>
<td>powersupply powersave</td>
<td></td>
</tr>
<tr>
<td>powersupply type</td>
<td></td>
</tr>
<tr>
<td>hash-control</td>
<td></td>
</tr>
<tr>
<td>bluetooth</td>
<td></td>
</tr>
<tr>
<td>capability profile</td>
<td></td>
</tr>
<tr>
<td>capability profile tcam mode</td>
<td></td>
</tr>
<tr>
<td>capability trap-threshold</td>
<td></td>
</tr>
<tr>
<td>capability shared-vlan-learning</td>
<td></td>
</tr>
<tr>
<td>uboot access</td>
<td></td>
</tr>
<tr>
<td>uboot authentication</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>capability trap-threshold</td>
<td></td>
</tr>
<tr>
<td>show system</td>
<td></td>
</tr>
<tr>
<td>show hardware-info</td>
<td></td>
</tr>
<tr>
<td>show chassis</td>
<td></td>
</tr>
<tr>
<td>show cmm</td>
<td></td>
</tr>
<tr>
<td>show slot</td>
<td></td>
</tr>
<tr>
<td>show module</td>
<td></td>
</tr>
<tr>
<td>show module long</td>
<td></td>
</tr>
<tr>
<td>show module status</td>
<td></td>
</tr>
<tr>
<td>show powersupply</td>
<td></td>
</tr>
<tr>
<td>show fan</td>
<td></td>
</tr>
<tr>
<td>show fantray</td>
<td></td>
</tr>
<tr>
<td>show temperature</td>
<td></td>
</tr>
<tr>
<td>show hash-control</td>
<td></td>
</tr>
<tr>
<td>show bluetooth status</td>
<td></td>
</tr>
<tr>
<td>show me</td>
<td></td>
</tr>
<tr>
<td>show team utilization</td>
<td></td>
</tr>
<tr>
<td>show team utilization detail</td>
<td></td>
</tr>
<tr>
<td>show team app-groups</td>
<td></td>
</tr>
<tr>
<td>show capability profile</td>
<td></td>
</tr>
<tr>
<td>show pmd-files</td>
<td></td>
</tr>
<tr>
<td>show tech-support</td>
<td></td>
</tr>
<tr>
<td>show capability trap-threshold</td>
<td></td>
</tr>
<tr>
<td>show mac-range</td>
<td></td>
</tr>
<tr>
<td>show mac-range alloc</td>
<td></td>
</tr>
<tr>
<td>show uboot config</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Licensing Commands</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>license apply file</td>
<td></td>
</tr>
<tr>
<td>show license-info</td>
<td></td>
</tr>
</tbody>
</table>
| Key Management Commands | security key-chain gen-random-key  
| security key  
| security key-chain  
| security key-chain key  
| show security key  
| show security key-chain |
| Alarm Relay Commands | alarm in  
| alarm event  
| alarm out  
| alarm map  
| alarm duration  
| alarm clear status  
| show alarm input config  
| show alarm event config  
| show alarm status |
| Application Manager Commands | appmgr  
| appmgr list  
| show appmgr (appmgr list)  
| pkgmgr  
| show pkgmgr (pkgmgr list)  
| pkgmgr commit  
| appmgr commit |
**system contact**

Specifies the administrative contact for the switch. An administrative contact is the person or department in charge of the switch. If a contact is specified, users can easily find the appropriate network administrator if they have questions or comments about the switch.

**system contact** *text_string*

---

**Syntax Definitions**

*text_string*  
The administrative contact being specified for the switch. The system contact can range from 1 to 254 characters in length. Text strings that include spaces must be enclosed in quotation marks. For example, “Jean Smith Ext. 477 jsmith@company.com”.

---

**Defaults**  
N/A

---

**Platforms Supported**  
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**  
N/A

---

**Examples**

-> system contact "Jean Smith Ext. 477 jsmith@company.com"
-> system contact engineering-test@company.com

---

**Release History**  
Release 7.1.1; command introduced.
Related Commands

- **system name**: Modifies the current system name of the switch.
- **system location**: Specifies the current physical location of the switch.
- **capability trap-threshold**: Displays the basic system information for the switch.

MIB Objects

- **system**
  - **systemContact**
**system name**

Modifies the current system name of the switch. The system name can be any simple, user-defined text description for the switch.

```
system name text_string
```

---

**Syntax Definitions**

`text_string`  
The new system name. The system name can range from 1 to 32 characters in length. No spaces are allowed in the system name.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Spaces are not allowed in the system name.
- The OmniSwitch can be configured with a DHCP client interface that allows the switch to dynamically obtain the system name (DHCP Option-12) from the DHCP server. The user-defined system name configuration (through CLI, WebView, SNMP) always gets priority over the DHCP server values. For more information on DHCP client options, refer to the “Configuring DHCP” chapter of the *OmniSwitch AOS Release 8 Network Configuration Guide*, and “IP Commands” chapter of the *OmniSwitch AOS Release 8 CLI Reference Guide*.

**Examples**

- `-> system name OmniSwitch6900`
- `-> system name OS6900`

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **system contact**: Specifies the administrative contact of the switch (for example, an individual or a department).
- **system location**: Specifies the current physical location of the switch.
- **capability trap-threshold**: Displays the basic system information for the switch.

MIB Objects

- **system**
  - **systemName**
**system location**

Specifies the current physical location of the switch. If you need to determine the location of the switch from a remote site, entering a system location can be very useful.

```
system location text_string
```

**Syntax Definitions**

`text_string`  
The physical location of the switch. For example, TestLab. The system location can range from 1 to 254 characters in length. Text strings that include spaces must be enclosed in quotation marks. For example, “NMS Test Lab”.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> system location "NMS Test Lab"
-> system location TestLab
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **system contact**: Specifies the administrative contact of the switch (for example, an individual or a department).
- **system name**: Modifies the current system name of the switch.
- **capability trap-threshold**: Displays the basic system information for the switch.

MIB Objects

- **system**
  - **systemLocation**
system date

Displays or modifies the current system date on the switch.

system date [mm/dd/yyyy]

Syntax Definitions

`mm/dd/yyyy` The new date being specified for the system. Enter the date in the following format: `mm/dd/yyyy`, where `mm` is the month, `dd` is the day, and `yyyy` is the year. For example, `08/08/2010`.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If you do not specify a new system date in the command line, the current system date is displayed.
- For more information on setting time zone parameters (for example, Daylight Savings Time), refer to the `system timezone` command on page 59-14.

Examples

-> system date 08/08/2010
-> system date
08/08/2010

Release History

Release 7.1.1; command introduced.
Related Commands

- **system time**  Displays or modifies the current system time on the switch.
- **system timezone**  Displays or modifies the time zone for the switch.

MIB Objects

- **systemServices**
  - **systemServicesDate**
system time

Displays or modifies the switch current system time.

**system time [hh:mm:ss]**

---

**Syntax Definitions**

`hh:mm:ss` The new time specified for the system. To set this value, enter the current time in 24-hour format, where `hh` is the hour, `mm` is the minutes, and `ss` is the seconds. For example, **14:30:00**.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a new system time is not specified in the command line, the current system time is displayed.
- Setting the year to 1970 is not supported. The system interprets 1970 as meaning the internal clock has never been set and will reset to the year 2014.
- The OmniSwitch 6360 does not contain a real-time clock.
  - It is recommended to use NTP to ensure time synchronization on an OmniSwitch 6360.
  - When the switch is reset, the switch will boot up from an approximation of the last known good time.
  - When the switch is powered off, it cannot detect the time left in the powered off state. When it boots up, it will have the same time as when the switch was last powered off.

**Examples**

```
-> system time 14:30:00
-> system time
14:30:08
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **system date**
  Displays or modifies the current system date on the switch.

- **system timezone**
  Displays or modifies the time zone for the switch.

MIB Objects

- **systemServices**
  - **systemServicesTime**
**system timezone**

Displays or modifies the time zone for the switch.

```plaintext
system timezone [timezone_abbrev]
```

### Syntax Definitions

**timezone_abbrev**

Specifies a time zone for the switch and sets the system clock to run on UTC. If a time zone abbreviation is specified, the hours offset from UTC is automatically calculated by the switch.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The configuration must be saved after changing the timezone.
- To display the current time zone for the switch, enter the syntax `system timezone`.
- If the configured timezone supports DST, it is automatically enabled and cannot be disabled.
- If the configured timezone does not support DST, it is automatically disabled and cannot be enabled.
- The OmniSwitch can be configured with a DHCP client interface that allows the switch to dynamically obtain the time zone (DHCP Option-2) from the DHCP server. The user-defined time zone configuration (through CLI, WebView, SNMP) always gets priority over the DHCP server values. For more information on DHCP client options, refer to the “Configuring DHCP” chapter of the *OmniSwitch AOS Release 8 Network Configuration Guide*, and “IP Commands” chapter of the *OmniSwitch AOS Release 8 CLI Reference Guide*.
- Refer to the *OmniSwitch AOS Release 8 Switch Management Guide* for a list of time zone abbreviations.

### Examples

```
-> system timezone mst
```

### Release History

Release 7.1.1; command introduced.
Related Commands

- **system date**
  Displays or modifies the current system date on the switch.

- **system time**
  Displays or modifies the current system time on the switch.

MIB Objects

- **systemServices**
  - systemServicesTimezone
  - systemServicesTimezoneStartWeek
  - systemServicesTimezoneStartDay
  - systemServicesTimezoneStartMonth
  - systemServicesTimezoneStartTime
  - systemServicesTimezoneOffset
  - systemServicesTimezoneEndWeek
  - systemServicesTimezoneEndDay
  - systemServicesTimezoneEndMonth
  - systemServicesTimezoneEndTime
  - systemServicesEnableDST
**system daylight-savings-time**

Displays the Daylight Savings Time (DST) setting for the configured timezone.

```
系统 daylight-savings-time [enable | disable]
```

---

**Syntax Definitions**

```
enable | disable
```

Enables or disables DST.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timezone supports DST</td>
<td>enabled</td>
</tr>
<tr>
<td>Timezone does not support DST</td>
<td>disabled</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- If the configured timezone supports DST it is automatically enabled.
- If the configured timezone does not support DST it is automatically disabled.

---

**Examples**

```
-> system daylight-savings-time
Daylight Savings Time (DST) is ENABLED.
```

---

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **system time** Displays or modifies the current system time on the switch.
- **system timezone** Displays or modifies the timezone for the switch.
- **system date** Displays or modifies the current system date on the switch.

MIB Objects

- **systemServices**
  - systemServicesTimezone
  - systemServicesEnableDST
update uboot

Updates the uboot versions of the CMM or NIs. Refer to the Release Notes and/or any available Upgrade Instructions for the new release before performing this type of update on the switch.

update uboot {cmm slot | ni {all | slot} file filename}

Syntax Definitions

- **cmm**: Specifies that the update is performed for the Chassis Management Module (CMM).
- **all**: Specifies that the update is performed for all slots within a chassis.
- **slot**: Specifies the slot number of the module within a chassis.
- **filename**: Specifies the path and name of the upgrade file.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Note that when performing an update, it is important that the correct update file is used. Specifying the wrong file may impact the operation of the switch.

Examples

- > update uboot ni all file 9999.tar.gz
- > update uboot cmm 1 file /flash/temp/9999.tar.gz

Release History

Release 7.1.1; command introduced.

Related Commands

- **reload slot**: Reloads the specified NI module.

MIB Objects

- **systemServices**:
  - systemServicesArg1
systemServicesAction
update fpga-cpld

Updates the FPGA/CPLD versions of the CMM or NIs. Refer to the Release Notes and/or any available Upgrade Instructions for the new release before performing this type of update on the switch.

update fpga-cpld \{cmm \{chassis/cmm |all\} | ni \{chassis/ni | daughter num\} file filename\}

**Syntax Definitions**

- **cmm**
  Specifies that the update is performed for the Chassis Management Module (CMM).

- **daughter**
  Specifies the number of the daughter board on the NI module.

- **ni**
  Specifies the slot number of the module within a chassis.

- **filename**
  Specifies the path and name of the upgrade file.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900 X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2/ X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Note that when performing an update, it is important that the correct update file is used. Specifying the wrong file may impact the operation of the switch.

- When updating CMMs with the **all** option an “fpga_kit” file must be used. If upgrading a CMM using the **chassis/cmm** option, a “vme” file must be used.

- A *.updater file can be used for upgrading ONIE-based devices.

- Refer to the appropriate release notes for release specific file information.

**Examples**

-> update fpga-cpld ni 4 file 9999.vme
-> update fpga-cpld cmm 1/1 file /flash/OS6865_U28X_CPLD_V11.vme
-> update fpga-cpld cmm all file fpga_kit_4960
-> update fpga-cpld cmm 1/1 file os6860n_p24m_p24z_maincpld_20220309.updater
**Release History**

Release 7.1.1; command introduced.
Release 7.3.4; **fpga** parameter changed to **fpga-cpld**.

**Related Commands**

- **reload slot**
  Reloads the specified NI module.

**MIB Objects**

- **systemServices**
  - **systemServicesArg1**
  - **systemServicesAction**
reload slot

Reloads or reboots a specified Network Interface (NI) module.

**reload slot slot**

---

**Syntax Definitions**

*slot* Specifies the slot number.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `reload slot` command reboots only the specified NI. Other modules installed on the chassis, including primary and secondary CMMs, are not affected.

**Examples**

```
-> reload slot 2
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **reload slot**: Reloads the specified NI module.
- **power slot**: Turns the power on or off for a specified NI module.
- **show slot**: Shows the hardware information and the current status for NI modules currently running in the chassis.

**MIB Objects**

- `chasEntPhysicalTable`
- `chasEntPhysAdminStatus`
- `reset`
power slot

Turns the power on or off for a specified Network Interface (NI) module.

`power slot chassis.slot`

`no power slot chassis.slot`

---

**Syntax Definitions**

`chassis`  
The chassis identifier.

`slot`  
The chassis slot number containing the NI module being powered on or off.

---

**Defaults**

N/A

---

**Platforms Supported**

Not supported in this release.

---

**Usage Guidelines**

Use the `no` form of this command to power off an NI module.

---

**Examples**

`-> power slot 1`
`-> power slot 7`

---

**Release History**

Release 7.1.1; command introduced.

---

**Related Commands**

`reload slot`  
Reloads the specified NI module.

`show slot`  
Shows the hardware information and current status for NI modules currently running in the chassis.

---

**MIB Objects**

`chasEntPhysicalTable`
`chasEntPhysAdminStatus`
`powerOn`
`powerOff`
powersupply enable

Enables the power supply unit identified by the PSU-ID.

powersupply enable [slot]

no powersupply enable [slot]

Syntax Definitions

slot Slot number of power supply.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

N/A

Release History

Release 7.1.1; command introduced.

Related Commands

power slot Turns the power on or off for a specified Network Interface (NI) module.

MIB Objects

N/A
powersupply powersave

Enables the power saving functionality on the switch.

`powersupply powersave {enable | disable}`

**Syntax Definitions**

| enable | disable | Enables or disables the power saving functionality. |

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

- When enabled unneeded power-supplies are shut down to conserve energy, only the power supplies required to provide N+1 redundancy remain on.

- If enabled and power is lost to all active power supplies simultaneously, the switch will lose power since N+1 redundancy applies only to the active power supplies.

- If the power-save mode is disabled, all available power supplies are switched on at all times.

**Examples**

```
-> powersupply powersave disable
-> powersupply powersave enable
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

show powersupply Displays the hardware information and current status for chassis power supplies.

**MIB Objects**

chasEntPhysicalTable
chasEntPhysAdminStatus
**powersupply type**

Configures the type of power supply that is connected to the chassis.

`powersupply num name string type {ALE {xl-ac | lo-ac | hi-ac} | phoenix-contact {48VDC | 24VDC} | third-party wattage num} [chassis-id chassis_id]`

---

**Syntax Definitions**

- `num` (power supply connector ID)
- `string` (the descriptive name of the power supply)
- `xl-ac | lo-ac | hi-ac` (the type of ALE power supply)
- `phoenix-contact 48VDC | 24VDC` (the type of Phoenix Contact power supply)
- `third-party wattage num` (the wattage value of the attached third-party power supply)

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The OmniSwitch 6465 cannot auto-detect the type of power supply connected. This command is used to configure the type of power supply that is connected.

- Refer to the OmniSwitch 6465 Hardware User Guide for chassis power requirements when using third-party power supplies.

- Refer to the OmniSwitch 6465 Hardware Users Guide for power supply specifications using the power supply part number mapping below. A power supply may be associated with multiple part numbers depending on ALE branding, ordering part number or manufacturer part number.
  - lo-ac (OS6465-BPN, PS-175AC, SDR-75-48)
  - hi-ac (O6465-BPN-H, PS-1185AC-P, SDR-240-55)
  - xl-ac (OS6465-BPN-X, PS-1275AC-P, SDR-480-48)

---

**Examples**

```
-> powersupply 1 name ALE-75W-ps1 type ale lo-ac
```
-> powersupply 2 name ALE-75W-ps2 type ale lo-ac
-> powersupply 1 name third-party-ps type third-party wattage 75

**Release History**

Release 8.5 R1; command introduced.

**Related Commands**

**show powersupply**

Displays the hardware information and current status for chassis power supplies.

**MIB Objects**

N/A
**hash-control**

Configures the hash control method on the switch. Depending upon this configuration, hashing algorithm used by various applications for packet forwarding is affected.

```
hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}
hash-control extended no udp-tcp-port
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>Sets hashing to brief mode.</td>
</tr>
<tr>
<td>extended</td>
<td>Sets hashing to extended mode.</td>
</tr>
<tr>
<td>udp-tcp-port</td>
<td>Sets extending hashing to use UDP/TCP ports.</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash-control</td>
<td>brief (OS6465, OS6900) extended (OS6560, OS6570M, OS6860, OS6865, OS9900)</td>
</tr>
<tr>
<td>udp-tcp-port</td>
<td>disabled</td>
</tr>
<tr>
<td>non-ucast</td>
<td>disabled</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Disabling TCP-UDP port hashing is recommended when Server Load Balancing (SLB) is configured, because SLB dynamically assigns ports.
- The hash control setting also impacts the fabric load balancing for Chassis based products. It is recommended not to set brief hashing mode on Chassis based products.
- Changing the hash control mode affects the hashing algorithm for Link Aggregation, Server Load Balancing and ECMP.
- The hashing mode must be set to extended to enable UDP/TCP port hashing.
• Enabling or disabling the **load-balance non-ucast** option applies to all link aggregates. When this option is disabled (the default), link aggregation load balances only unicast packets; all non-unicast packets are sent through the primary port of the link aggregate.

• When the **load-balance non-ucast** option is enabled, all non-unicast traffic (broadcast, L2 multicast, L3 multicast, and unknown unicast) is load balanced over the link aggregate.

**Examples**

-> hash-control brief  
-> hash-control extended  
-> hash-control extended udp-tcp-port  
-> hash-control extended no udp-tcp-port  
-> hash-control load-balance non-ucast enable  
-> hash-control load-balance non-ucast disable

**Release History**

Release 7.2.1; command introduced.

**Related Commands**

`show hash-control` Displays the current hash control setting for the switch.

**MIB Objects**

alaChasHashMode  
alaChasUdpTcpPortMode  
alachasNonUCHashControl
**bluetooth**

Enables or disables USB adapter with Bluetooth technology connectivity and configures the power level.

`bluetooth {admin-state [enable | disable] | transmit-power [low | high]}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>enable</th>
<th>disable</th>
<th>Enables or disables USB adapter with Bluetooth technology connectivity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>high</td>
<td>Configures the power level to low or high.</td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
<tr>
<td>low</td>
<td>high</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command will configure all USB adapters with Bluetooth technology in a virtual chassis.

**Examples**

- `-> bluetooth admin-state enable`
- `-> bluetooth transmit-power high`

**Release History**

Release 8.1.1; command was introduced.
Related Commands

- **show bluetooth status**  
  Displays the current USB adapter with Bluetooth technology settings.

- **show me**  
  Executes an LED blink pattern for 10 seconds that is used by the USB adapter with Bluetooth technology to identify the connected switch.

MIB Objects

- **systemServices**
  - **systemServicesUsbEnable**
  - **systemServicesBluetoothTxPower**
**capability profile**

Configures the mode of the switch to be either *switch* or *router*.

```
capability profile {switch | router}
```

**Syntax Definitions**

- `switch | router`: Configures the *switch* or *router* profile.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch</td>
<td>router</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72 Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6465</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6560</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to change the mode of a switch between *switch* and a *router*. This will adjust the L2 and L3 table entries based on the network requirements.

- The *switch* profile provides more L2 entries. The *router* profile provides more LPM entries. Refer to the Specifications Guide for details on the L2 and L3 entries.

- The switch must be rebooted for the configured profile to take effect.

**Examples**

```
-> capability profile router
```

**Release History**

Release 8.5R2; command was introduced.
**Related Commands**

- `show capability profile` Displays the active and configured profile settings.

**MIB Objects**

<table>
<thead>
<tr>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>alaCapManProfile</td>
</tr>
<tr>
<td>alaCapManProfileMode</td>
</tr>
</tbody>
</table>
**capability profile tcam mode**

Configures the TCAM (Ternary Content Addressable Memory) mode of the switch to support source IPv6 filtering.

`capability profile tcam mode {source-ipv6 | dest-ipv6}`

**Syntax Definitions**

- `source-ipv6` Selects the source IPv6 (enhanced) mode.
- `dest-ipv6` Selects the destination IPv6 mode.

**Defaults**

By default, the TCAM mode supports destination IPv6 filtering only; source IPv6 filtering is not allowed.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Setting the TCAM mode to source IPv6 filtering is required to support DHCPv6 Snooping IPv6 source filtering on an OmniSwitch 6560 and OmniSwitch 6570M.
- When the TCAM mode is changed, a warning message is displayed (see command examples below).
- After the TCAM mode is changed and the configuration is saved with the `write memory` command, reboot the switch to activate the specified mode.
- When the TCAM mode is set to source IPv6 filtering, the TCAM will operate in an enhanced mode to support the use of source IPv6 conditions in QoS policy rules.
- The following functionality is not supported when the source IPv6 filtering mode is active:
  - Destination IPv6 source filtering.
  - ISSU
  - QoS anti-spoofing
  - Fewer QoS policy rules supported.

**Examples**

```
-> capability profile tcam mode source-ipv6
WARNING: Source ipv6 tcam mode would not support : QoS policy with destination ipv6 address / destination network group / ipv6 Tcpflags. Reboot is needed for the capability profile tcam mode to use source-ipv6
```
capability profile tcam mode dest-ipv6
WARNING: Destination ipv6 tcam mode would not support : QoS policy with source ipv6 address / source network group.
Reboot is needed for the capability profile tcam mode to use dest-ipv6

Release History
Release 8.6R1; command was introduced.

Related Commands

`dhcppv6-snooping ipv6-source-filter`  
Confirms the IPv6 source filtering capability for a port, link aggregate, or VLAN using the DHCPv6 Snooping binding table.

`show tcam utilization detail`  
Displays additional TCAM usage information, such as application usage.

`show capability profile`  
Displays the active and configured profile settings.

MIB Objects

alaCapManProfile

alaCapManProfileTcamMode
capability trap-threshold

Configures the MAC and ARP table utilization high and low values for generating the associated traps.

```
capability trap-threshold {MAC | ARP} {HIGH num | LOW num}
```

**Syntax Definitions**

- **MAC**: Configures the MAC table threshold.
- **ARP**: Configures the ARP table threshold.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH num</td>
<td>95</td>
</tr>
<tr>
<td>LOW num</td>
<td>90</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the table utilization reaches the configured HIGH value a trap will be sent indicating the usage has reached the HIGH value. The trap will continue to be periodically sent until the usage drops below the configured HIGH value.
- Once the usage drops to the configured LOW value, a trap will be sent indicating the usage has dropped below the configured LOW value.
- The minimum LOW value is 5% and the maximum HIGH value is 95%. It is recommended to have a difference of at least 5% between LOW and HIGH values.

**Examples**

- `-> capability trap-threshold ARP HIGH 90 LOW 80`
- `-> capability trap-threshold MAC HIGH 88 LOW 80`

**Release History**

Release 8.6R1; command was introduced.
Related Commands

show capability trap-threshold  Displays the capability trap-threshold configured values.

MIB Objects

alaCapManTrapThreshold
   alaCapManTrapThresholdMacLow
   alaCapManTrapThresholdMacHigh
   alaCapManTrapThresholdArpLow
   alaCapManTrapThresholdArpHigh
capability shared-vlan-learning

Enables or disables shared VLAN learning. When enabled (the default), this functionality provides system resources for a Private VLAN (PVLAN) configuration.

capability shared-vlan-learning {enable | disable}

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Shared VLAN learning is enabled to support PVLAN configuration.</td>
</tr>
<tr>
<td>disable</td>
<td>Shared VLAN learning is disabled to free up system resources. PVLAN configuration is not available.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

Platforms Supported

Not supported in this release.

Usage Guidelines

A switch reboot is required whenever shared VLAN learning is enabled or disabled.

Examples

- `-> capability shared-vlan-learning disable`
- `-> capability shared-vlan-learning enable`

Release History

Release 8.7R2; command introduced.

Related Commands

- `show pvlan` Displays a list of PVLANs configured on the switch.

MIB Objects

alaCapManSharedVlanLearningConfig
alaCapManSharedVlanLearning
**uboot access**

Enables or disables the U-boot access.

`uboot access {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td>Enable the U-boot access.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>Disable the U-boot access.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, U-boot access is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>No</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>No</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>No</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Only the admin user can enable or disable the U-boot access.
- When the U-boot access is enabled, U-boot shell can be accessed with any key-press at AOS boot.
- When the U-boot access is disabled, any key-press at AOS boot does not allow access to U-boot shell. AOS images are booted with the pre-set parameters. If the AOS images are not valid or corrupted, switch goes to no response state, where only watch-dog reboots are possible. U-boot cannot start AOS and recover options cannot be used, as these options need U-boot access. In this case, the switch must be returned to the factory for repair as it cannot be recovered by the admin user.
- In case of VC, U-boot access configuration shall be synched to all the units of VC. The U-boot access configuration shall not be synched to any new unit (slave) joining the VC later. The U-boot access configuration must be applied before the new slave joins the VC or reapplied on the VC master after the new slave joins the VC.
- U-boot authentication feature does not have any effect, when U-boot access is disabled. When U-boot access enabled, it takes the latest authentication status.

**Examples**

```
-> uboot access enable
-> uboot access disable
```
Release History
Release 8.7R3; command introduced.

Related Commands
- `uboot authentication`  Enables or disables the U-boot authentication.
- `show uboot config`     Displays the U-boot authentication status.

MIB Objects
- `alaAaaU-bootAccess`
**uboot authentication**

Enables or disables the U-boot authentication.

`uboot authentication {enable password password | disable}`

---

### Syntax Definitions

- **enable**
  - Enable the U-boot authentication.

- **disable**
  - Disable the U-boot authentication.

- **password**
  - The U-boot password. The password can be between 8 to 30 characters.

---

### Defaults

By default, U-boot authentication is disabled.

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- When the authentication option is enabled, password input must be given. The U-boot shell is allowed to access only after authenticating with the password.

- Maximum of five retirees are allowed for the U-boot password. If the user enters the wrong password for five times, U-boot will proceed with the normal AOS boot.

- U-boot does not prompt for the password if AOS has not enabled the U-boot authentication with a password.

- The U-boot password cannot be modified at the U-boot prompt. Only the admin user can modify or set the password using the U-boot authentication command. If the user forgets the password, user can continue to normal AOS boot. The admin user can then modify or reset the U-boot password.

- In case of VC, the U-boot authentication password must be applied before the new slave joins the VC or reapplied on the VC master after the new slave joins the VC.

---

### Examples

- `-> uboot authentication enable password abcd1234`
- `-> uboot authentication disable`

---

### Release History

Release 8.7R3; command introduced.
Related Commands

- **uboot access**  Enables or disables the U-boot access.
- **show uboot config**  Displays the U-boot authentication status.

MIB Objects

- alaAaaUbootAuthenticationPassword
license apply file

Activates the license for licensed protocols on the switch.

```
license apply {file file_name | key license_key} [order-id order_id]
```

**Syntax Definitions**

- `file_name`: The name of the license file containing the license keys.
- `license_key`: Enter the individual license key. The license key can contain special characters; it is required to encase using single quote character ("'). The `key` input is needed only for applying MACsec license.
- `order_id`: The order ID for the MACsec license.

**Defaults**

By default, licensed protocols are not activated on the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td>T48C6/T48C6</td>
<td>X48C4E/X48C8</td>
<td>C32E/T24C2</td>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The license file can have any name.
- The license file is only used to activate the licensed features and does not need to remain on the switch.
- Using `key` option, the license key can be directly entered in the command. The license key can contain special characters; it is required to encase the key using single quote character ("'). The `key` input is needed only for applying MACsec license.
- Performance software license (OS6560-SW-PERF) is optional allowing ports 25/26 (OS6560-24X4/P24X4) and ports 49/50 (OS6560-48X4/P48X4) to operate at 10G speed. Ports support 1G by default. There is no reboot required after applying this license, but the ports should be administratively disabled and re-enabled.
- Performance software license (OS6360-SW-PERF) is optional allowing the two RJ45/SFP+ combo ports (25/26) of the OS6360-PH24 model to operate at 10G speed. Ports support 1G by default. There is no reboot required after applying this license, but the ports should be administratively disabled and re-enabled.
- The module type will continue to display as ‘U16L’ even after upgrading a ‘U16’ to a ‘U16E’.
- The `order-id` parameter is mandatory for MACsec license but it is not applicable for other licenses.
- The MACsec license is a site license and does not use the serial number and the MAC address of the switch. However, `order-id` is required for the license generator to generate MACsec license. The order ID value entered in this command is validated against the order ID in the license file. If this value does not match with the value stored in license file, MACsec license will not be installed.

- The order ID is a seven digit number and the license generation process appends the digit 0 at the beginning implicitly. Hence, it is required to provide eight digits (0 + 7 digits of the order ID) to install the license successfully.

- The Metro license is created based on the generic Metro type (feature ID), this is based on MAC address and the serial number of the unit.

- Following features are part of Metro license: CPE Test Head, PPPoE-IA, Ethernet OAM, SAA, Link OAM, VLAN Stacking, Dynamic Proxy ARP, Hardware Loopback. Metro license is required to configure these features on the switch.

- The Metro license is applicable for all OmniSwitch 6560 and OmniSwitch 6570M, which support Metro feature. The Metro configuration will be rejected if the Metro license is not installed prior to configuration. On other platforms, Metro features does not require a license.

- The switch must be rebooted to reflect the licensed feature set. For MACsSec, 10G license, and Metro license, a reboot is not required.

**Examples**

```
-> license apply file /flash/swlicense.txt
The switch will reboot after the license is applied.
Are you sure you want to proceed(Y/N)?Y
```

```
-> license apply file \flash\swlicense.dat order-id "07766551"
```

```
-> license apply key 'hasJ-i{v!-[qVW-YPr-t@YK' order-id "01234567"
```

**Release History**

Release 7.2.1; command was introduced.
Release 7.3.1; `key` and `deactivate` parameters deprecated.
Release 8.6R1; MACsec site-wide license and OmniSwitch 6560 10-Gigabit port license support added.
Release 8.6R2; `key` parameter added.
Release 8.9R1; Metro license support added for OmniSwitch 6560.

**Related Commands**

`show license-info` Displays all the licensed applications installed on the switch.

**MIB Objects**

- `alaCapManVcSwLicensingAction`
- `alaCapManVcSwLicensingActionArg`
- `alaCapManVcSwLicensingOrderId`
show system

Displays basic system information for the switch. Information includes a user-defined system description, name, administrative contact, location, object ID, up time, and system services.

show system

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples

-> show system
System:
    Description: Alcatel-Lucent Enterprise OS6900-X40 8.3.1.313.R01 GA, August 31, 2016.,
    Object ID: 1.3.6.1.4.1.6486.801.1.2.1.10.1.2,
    Up Time:   2 days 1 hours 32 minutes and 40 seconds,
    Contact:   Alcatel-Lucent, http://enterprise.alcatel-lucent.com,
    Name:      (none),
    Location:  Unknown,
    Services:  78,
    Date & Time: FRI OCT 07 2016 14:10:02 (UTC)
Flash Space:
    Primary CMM:
        Available (bytes): 856936448,
        Comments : None

output definitions

System Description The description for the current system. This description shows the current software version and the system date.

System Object ID The SNMP object identifier for the switch.
### System Up Time
The amount of time the switch has been running since the last system reboot.

### System Contact
An user-defined administrative contact for the switch. This field is modified using the `system contact` command.

### System Name
A user-defined text description for the switch. This field is modified using the `system name` command.

### System Location
The user-defined physical location of the switch. This field is modified using the `system location` command.

### System Services
The number of current system services.

### System Date & Time
The current system date and time. This field is modified using the `system date` and `system time` commands.

### Flash Space: Primary CMM:
#### Available (bytes)
The available flash memory space available on the primary management module of the switch.

### Flash Space: Primary CMM:
#### Comments
Comments regarding the available flash memory space available on the primary management module of the switch, if applicable.

### Release History
Release 7.1.1; command introduced.

### Related Commands
- **system contact**: Specifies the administrative contact for the switch (for example, an individual or a department).
- **system name**: Modifies the current system name of the switch.
- **system location**: Modifies the current physical location of the switch.

### MIB Objects
```
system
  systemContact
  systemName
  systemLocation
```
**show hardware-info**

Displays the current system hardware information. Includes CPU, flash, RAM, NVRAM battery, jumper positions, BootROM, and miniboost and FPGA information.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The fields displayed may differ slightly based on the switch model. The example given is for an OS9900.

**Examples**

```
-> show hardware-info
Chassis 1
CPU Manufacturer : GenuineIntel
CPU Model         : Intel(R) Atom(TM) CPU C2518 @ 1.74GHz
Compact Flash Manufacturer : MICRON
Compact Flash size   : 1997967360 bytes
RAM Manufacturer    : Micron
RAM size            : 16322816kB
Control FPGA version : 2.0.0
Power FPGA version   : 0.8
Coreboot Version     : 8.3.1.103.R01
CPMs Present         : 1,-
Power Supplies Present: 1,2,-
Fan Trays Present    : 1,2,3
NIs Present          : 1,-,3,4,-,-,-
```

**output definitions**

- **CPU Manufacturer**: The manufacturer of the CPU used on the CMM.
- **CPU Model**: The model of the CPU on the CMM.
- **Compact Flash Manufacturer**: The manufacturer of the flash memory used on the CMM.
Chassis Management and Monitoring Commands

show hardware-info

output definitions (continued)

<table>
<thead>
<tr>
<th>Compact Flash size</th>
<th>The total amount of flash memory (file space) on the CMM. This field specifies the total flash memory size only and does not indicate the amount of memory free or memory used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM Manufacturer</td>
<td>The manufacturer of the RAM memory used on the CMM.</td>
</tr>
<tr>
<td>RAM size</td>
<td>The total amount of RAM memory on the CMM. This field specifies the total RAM memory only and does not indicate the amount of memory free or memory used.</td>
</tr>
<tr>
<td>Control FPGA version</td>
<td>The version of the control FPGA on the CMM.</td>
</tr>
<tr>
<td>Power FPGA version</td>
<td>The version of the power FPGA on the CMM.</td>
</tr>
<tr>
<td>Coreboot Version</td>
<td>The version of the Coreboot on the CMM.</td>
</tr>
<tr>
<td>CFMs Present</td>
<td>The number of CFMs in the chassis.</td>
</tr>
<tr>
<td>Power Supplies Present</td>
<td>The number of power supplies in the chassis.</td>
</tr>
<tr>
<td>Fan Trays Present</td>
<td>The number of fan trays in the chassis.</td>
</tr>
<tr>
<td>NIs Present</td>
<td>The number of NIs in the chassis.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

show chassis
Displays the basic configuration and status for the switch chassis.

show cmm
Displays the basic hardware and status information for CMM modules running in the chassis.

MIB Objects

systemHardware
  systemHardwareFlashMfg
  systemHardwareFlashSize
  systemHardwareMemoryMfg
  systemHardwareMemorySize
  systemHardwareNVRAMBatteryLow
  systemHardwareBootCpuType
  systemHardwareJumperInterruptBoot
  systemHardwareJumperForceUartDefaults
  systemHardwareJumperRunExtendedMemoryDiagnostics
  systemHardwareJumperSpare
  systemHardwareFpgaVersionIndex
  systemHardwareFpgaVersion
  systemHardwareBootRomVersion
  systemHardwareDefaultMiniBootVersion
  systemHardwareBackupMiniBootVersion
  systemHardwareCpldVersion
  systemHardwareMinorFpgaVersion
  systemHardwareProdRegId
  systemHardwareRevisionRegister
  systemHardwareUbootMinibootVersion
  systemHardwareUbootVersion
  systemHardwareXfpId
**show chassis**

Displays the basic configuration and status information for the switch chassis.

```
show chassis
```

---

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

| Model | Supported
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C4E/V48C8</td>
<td>Yes</td>
</tr>
<tr>
<td>C32E/T24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show chassis
Local Chassis ID 1 (Master)
  Model Name: OS9900,
  Description: Chassis,
  Part Number: 903722-90,
  Hardware Revision: B,
  Serial Number: T4720029,
  Manufacture Date: Feb 1 2016,
  Admin Status: POWER ON,
  Operational Status: UP,
  Free Slots: 4,
  Power Left: 1540,
  Number Of Resets: 28,
  MAC Address: 2c:fa:a2:13:e4:02
```

---

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>The factory-set model name for the switch. This field cannot be modified.</td>
</tr>
<tr>
<td>Description</td>
<td>The factory-set description for the switch. This field cannot be modified.</td>
</tr>
<tr>
<td>Part Number</td>
<td>The part number for the chassis.</td>
</tr>
</tbody>
</table>
Release History
Release 7.1.1; command introduced.

Related Commands

- **show hardware-info**
  Displays the current system hardware information.

- **show powersupply**
  Displays the hardware information and current status for chassis power supplies.

- **show fan**
  Displays the current operating status of chassis fans.

MIB Objects

- **chasChassisTable**
- **chasFreeSlots**
- **chasPowerLeft**
**show cmm**

Displays basic hardware and status information for the CMM modules in a standalone switch.

`show cmm [slot]`

---

**Syntax Definitions**

| `slot` | Specifies the CMM by slot number or letter. |

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

On chassis-based switches, a CMM installed in the left CMM slot position is defined as CMM-A. A CMM installed in the right position is CMM-B.

**Examples**

```
-> show cmm
Chassis ID 1 Module in slot CMM-A
    Model Name:    OS99-CMM,
    Module Type:   0x7100101,
    Description:   MGMT MODULE,
    Part Number:   903754-90,
    Hardware Revision: C06,
    Serial Number: U1820028,
    Manufacture Date: May 10 2016,
    FPGA - Control: 2.0.0,
    FPGA - Power:   0.8,
    Admin Status:   POWER ON,
    Operational Status: UP,
    Max Power:       64,
    CPU Model Type:  Intel Atom C2518,
    MAC Address:    2c:fa:a2:13:e4:02,
    Coreboot Version: 8.3.1.103.R01
```

**output definitions**

<table>
<thead>
<tr>
<th>Model Name</th>
<th>The model name of the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Type</td>
<td>A unique module ID specific to the type of module.</td>
</tr>
</tbody>
</table>
### Output Definitions (continued)

<table>
<thead>
<tr>
<th>Description</th>
<th>A factory-defined description of the associated board.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part Number</td>
<td>The part number for the board.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>The hardware revision level for the board.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number for the board.</td>
</tr>
<tr>
<td>Manufacture Date</td>
<td>The date the board was manufactured.</td>
</tr>
<tr>
<td>FPGA - Control</td>
<td>FPGA version.</td>
</tr>
<tr>
<td>FPGA - Power</td>
<td>FPGA version</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The current power status of the CMM. Information is obtained from a running CMM. Hence the value is always POWER ON.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The current operational status of the CMM.</td>
</tr>
<tr>
<td>Max Power</td>
<td>The maximum power for the CMM.</td>
</tr>
<tr>
<td>CPU Model Type</td>
<td>The CPU Model type.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address assigned to the chassis.</td>
</tr>
<tr>
<td>Coreboot Version</td>
<td>The boot version number for the CMM.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command introduced.

### Related Commands

- **show chassis**
  Displays the basic configuration and status information for the switch chassis.

- **show slot**
  Displays the basic hardware and status information for Network Interface (NI) modules currently installed in the switch.

- **show module**
  Displays the basic information for either a specified module or all the modules installed in the chassis.

- **show module long**
  Displays the detailed information for either a specified module or all modules installed in the chassis.

- **show module status**
  Displays the basic status information for either a specified module or all modules installed in the chassis.

- **capability trap-threshold**
  Displays the status and configuration of Switch Fabric Modules (SFMs) on chassis-based switches.

### MIB Objects

N/A
show slot

Displays the basic hardware and status information for Network Interface (NI) modules currently installed in the chassis.

**show slot [slot]**

---

**Syntax Definitions**

**slot**

The slot number for a specific NI module installed in the chassis. If no slot number is specified, information for all the NI modules is displayed.

---

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

When this command is entered from the secondary CMM, the Operational and Admin Status for NIs will display as ‘UNKNOWN’.

---

**Examples**

```
-> show slot 1
Module in slot 1
  Model Name: OS10-GNI-C48,
  Description: 10-1000 RJ45,
  Part Number: 902434-90,
  Hardware Revision: A07,
  Serial Number: H03Q0008,
  Manufacture Date: JAN 31 2007,
  FPGA - Physical 1: 007,
  Daughter FPGA - Physical 1: 002,
  Daughter FPGA - Physical 2: 002,
  Admin Status: POWER ON,
  Operational Status: UP,
  Power Consumption: 200,
  CPU Model Type: Motorola MPC854
  MAC Address: 00:0d:09:50:01:04:
  ASIC - Physical 1: BCM56620_A1,
  ASIC - Physical 2: BCM56620_A1,
  ASIC - Physical 3: BCM56620_A1,
  ASIC - Physical 4: BCM56620_A1,
```
Chassis Management and Monitoring Commands

<table>
<thead>
<tr>
<th>ASIC - Physical 5:</th>
<th>BCM56620_A1,</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIC - Physical 6:</td>
<td>BCM56620_A1,</td>
</tr>
<tr>
<td>UBOOT Version:</td>
<td>7.1.1.412.R01,</td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Model Name</th>
<th>The NI module name. For example, OS9-GNI-C24 indicates a twenty-four-port 10/100/1000BaseT Ethernet module.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A general description of the NI. For example, 24pt 10/100/1000BaseT Mod indicates a twenty-four-port 10/100/1000BaseT Ethernet module.</td>
</tr>
<tr>
<td>Part Number</td>
<td>The part number for the NI.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>The hardware revision level for the NI.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number for the NI printed circuit board (PCB).</td>
</tr>
<tr>
<td>Manufacture Date</td>
<td>The date the NI was manufactured.</td>
</tr>
<tr>
<td>FPGA/Daughter FPGA</td>
<td>The FPGA versions.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The current power status of the NI. Options include POWER ON or POWER OFF.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The operational status of the NI. Options include UP or DOWN. The operational status can be DOWN while the power status is on, indicating a possible software issue.</td>
</tr>
<tr>
<td>Power Consumption</td>
<td>The current power consumption for the module.</td>
</tr>
<tr>
<td>CPU Model Type</td>
<td>The CPU model type.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address assigned to the NI.</td>
</tr>
<tr>
<td>ASIC - Physical</td>
<td>General information regarding the NI module ASICs.</td>
</tr>
<tr>
<td>UBOOT Version</td>
<td>UBOOT version of the NI.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

reload slot  Reloads the specified NI module.

power slot  Turns the power on or off for a specified Network Interface (NI) module.

show module  Displays the basic information for either a specified module or all modules installed in the chassis.

show module long  Displays the detailed information for either a specified module or all modules installed in the chassis.

show module status  Displays the basic status information for either a specified module or all modules installed in the chassis.

MIB Objects

chasEntPhysOperStatus
show module

Displays the basic information for either a specified module or all modules installed in a standalone switch chassis.

show module [slot]

Syntax Definitions

slot

The slot number or CMM letter for a specific module installed in the chassis. If no slot number is specified, information for all modules is displayed.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C4E/V48C8/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900C32E/T24C2/</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show module

<table>
<thead>
<tr>
<th>Slot</th>
<th>Part-Number</th>
<th>Serial #</th>
<th>HW Rev</th>
<th>Mfg Date</th>
<th>Model Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMM-A</td>
<td>902271-10</td>
<td>E23L9059</td>
<td>002 JUN 08 2004</td>
<td>OS10-CPM</td>
<td></td>
</tr>
<tr>
<td>SLOT-1</td>
<td>902271-10</td>
<td>E23L9059</td>
<td>002 JUN 08 2004</td>
<td>OS10-GNI-C48</td>
<td></td>
</tr>
</tbody>
</table>

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot</td>
<td>The chassis slot position of the module.</td>
</tr>
<tr>
<td>Part-Number</td>
<td>The part number for the module.</td>
</tr>
<tr>
<td>Serial #</td>
<td>The serial number for the module.</td>
</tr>
<tr>
<td>Rev</td>
<td>The hardware revision level for the module.</td>
</tr>
<tr>
<td>Date</td>
<td>The date the module was manufactured.</td>
</tr>
<tr>
<td>Model Name</td>
<td>The descriptive name for the module.</td>
</tr>
</tbody>
</table>
## Release History

Release 7.1.1; command introduced.

## Related Commands

- **show module long**
  
  Displays the detailed information for either a specified module or all modules installed in the chassis.

- **show module status**
  
  Displays the basic status information for either a specified module or all modules installed in the chassis.

## MIB Objects

- **N/A**
**show module long**

Displays the detailed information for either a specified module or all the modules installed in a standalone switch chassis.

**show module long [slot]**

---

**Syntax Definitions**

*slot*  
The slot number or CMM letter for a specific module installed in the chassis. If no slot number is specified, information for all modules is displayed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

**Examples**

```
-> show module long 1
Module in slot 1
Model Name:                    OS99-GNI-P48,
Module Type:                   0x70e2101
Description:                   48 G POE,
Part Number:                   903726-90,
Hardware Revision:             A07,
Serial Number:                 H03Q0008,
Manufacture Date:              JAN 31 2007,
FPGA - Control                 1.2.4,
FPGA - Power                   0.9
Daughter FPGA - Physical 1:    002,
Daughter FPGA - Physical 2:    002,
Admin Status:                  POWER ON,
Operational Status:            UP,
Max Power:                     54,
CPU Model Type :               Intel Atom C2338
MAC Address:                   00:d0:95:01:04:
ASIC - Physical 1:            BCM56620_A1,
ASIC - Physical 2:            BCM56620_A1,
```
### ASIC - Physical
- ASIC - Physical 3: BCM56620_A1
- ASIC - Physical 4: BCM56620_A1
- ASIC - Physical 5: BCM56620_A1
- ASIC - Physical 6: BCM56620_A1
- UBOOT Version: 7.1.1.412.R01
- POE-Software Version: PD69100 Software Version 00.0255.01 Hardware Version 00 NI 1

---

### output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>The NI module name.</td>
</tr>
<tr>
<td>Description</td>
<td>A general description of the NI.</td>
</tr>
<tr>
<td>Part Number</td>
<td>The part number for the NI.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>The hardware revision level for the NI.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number for the NI printed circuit board (PCB).</td>
</tr>
<tr>
<td>Manufacture Date</td>
<td>The date the NI was manufactured.</td>
</tr>
<tr>
<td>FPGA/Daughter FPGA</td>
<td>The FPGA versions.</td>
</tr>
<tr>
<td>Admin Status</td>
<td>The current power status of the module. Options include POWER ON or POWER OFF.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The operational status of the module. Options include UP or DOWN. The operational status can be DOWN while the power status is on, indicating a possible software issue.</td>
</tr>
<tr>
<td>Max Power</td>
<td>The maximum power consumption for the module.</td>
</tr>
<tr>
<td>CPU Model Type</td>
<td>The CPU model type.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address assigned to the module.</td>
</tr>
<tr>
<td>ASIC - Physical</td>
<td>General information regarding the module ASICS.</td>
</tr>
<tr>
<td>UBOOT Version</td>
<td>UBOOT version of the module.</td>
</tr>
<tr>
<td>POE-Software Version</td>
<td>The PoE controller firmware/hardware revision.</td>
</tr>
</tbody>
</table>

---

### Release History
Release 7.1.1; command introduced.

### Related Commands

- **show module**
  - Displays the basic information for either a specified module or all modules installed in the chassis.

- **show module status**
  - Displays the basic status information for either a specified module or all modules installed in the chassis.

### MIB Objects

- **N/A**
show module status

Displays the basic status information for either a specified module or all modules installed in a standalone switch chassis.

show module status [slot]

Syntax Definitions

slot

The slot number or CMM letter for a specific module installed in the chassis. If no slot number is specified, information for all modules is displayed.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

When this command is entered from the secondary CMM, the Operational and Admin Status for NIs will display as ‘UNKNOWN’.

Examples

-> show module status

<table>
<thead>
<tr>
<th>Slot</th>
<th>Operational Status</th>
<th>Admin-Status</th>
<th>Rev</th>
<th>MAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMM-A</td>
<td>UP</td>
<td>POWER ON</td>
<td>N/A</td>
<td>00:d0:95:a3:e5:09</td>
</tr>
<tr>
<td>SLOT-1</td>
<td>UP</td>
<td>POWER ON</td>
<td>N/A</td>
<td>00:d0:95:a3:e5:0b</td>
</tr>
</tbody>
</table>

output definitions

Slot

The chassis slot position of the module. For detailed slot numbering information, refer to the “Chassis and Power Supplies” chapter of the Hardware User Guide. Refer to page 59-51 for additional information on CMM callouts.

Operational Status

The operational status of the module. Options include UP or DOWN. For NI and secondary CMM modules, the operational status can be DOWN while the power status is on, indicating a possible software issue.
### Output Definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin-Status</strong></td>
<td>The current power status of the module. Options include POWER ON or POWER OFF.</td>
</tr>
<tr>
<td><strong>Firmware Rev</strong></td>
<td>The firmware version for module ASICs.</td>
</tr>
<tr>
<td><strong>MAC</strong></td>
<td>For the CMM, the base chassis MAC address is displayed. For NI modules, the MAC address for the corresponding NI is displayed.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command introduced.

### Related Commands

- **show module**
  - Displays the basic information for either a specified module or all the modules installed in the chassis.

- **show module long**
  - Displays the detailed information for either a specified module or all the modules installed in the chassis.

### MIB Objects

| N/A |
**show powersupply**

Displays the hardware information and current status for chassis power supplies.

`show powersupply [slot]`

### Syntax Definitions

- **slot**
  - The slot number for a specific power supply installed in the chassis. If no power supply number is specified, information for all power supplies is displayed.

- **powersave status**
  - Displays the status of the power saving functionality.

### Defaults

The OmniSwitch 6465 and 6570 cannot auto-detect the type of power supply connected and will not display a power supply that is not powered up. Use the `powersupply type` command on the OS6465 to manually configure a power supply.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show powersupply
+---+-----+-------+--------+---------+--------+--------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+----------+-----------
Chassis Management and Monitoring Commands

---+----+---------+--------+--------+-----------+-----------+-----------
 | 1  | 450 | 201    | AC     | UP      | Internal   | Front to Rear |
 | 2  | 450 | 50     | AC     | UP      | Internal   | Front to Rear |

-> show powersupply 1

Module in slot PS-1
Model Name: YM-2451DDR,
Module Type: DC/DC Power Supply, Front to Rear Airflow
Description: OS-PS-450W-D
Hardware Revision: B0,
Serial Number: 1020000417,
Manufacture Date: May 14 2010,
Operational Status: UP,
Power Provision: 450W

---

**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>The power supply model number.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the associated power supply. This field reflects the model name in most cases.</td>
</tr>
<tr>
<td>Part Number</td>
<td>The part number for the power supply.</td>
</tr>
<tr>
<td>Hardware Revision</td>
<td>The hardware revision level for the power supply.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number for the power supply.</td>
</tr>
<tr>
<td>Manufacture Date</td>
<td>The date the power supply was manufactured.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The operational status of the power supply. Options include UP or DOWN.</td>
</tr>
<tr>
<td>Power Provision</td>
<td>The number of watts provided by this power supply.</td>
</tr>
<tr>
<td>PS</td>
<td>The slot number of the power supply.</td>
</tr>
<tr>
<td>Total Power</td>
<td>The number of watts provided by this power supply.</td>
</tr>
<tr>
<td>Power Used</td>
<td>The number of watts being used by this power supply.</td>
</tr>
<tr>
<td>Input Voltage</td>
<td>The input line voltage of this power supply.</td>
</tr>
<tr>
<td>PS type</td>
<td>The type of power supply. AC or DC.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>The operational status of the power supply. Options include UP, DOWN, or UNPLUG.</td>
</tr>
<tr>
<td>Location</td>
<td>The location of the power supply. Options include Internal or External.</td>
</tr>
<tr>
<td>Slots 5-8 are for the optional power shelf.</td>
<td></td>
</tr>
<tr>
<td>Airflow</td>
<td>Direction of airflow.</td>
</tr>
</tbody>
</table>

---

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **show chassis**
  Displays the basic configuration and status information for the switch chassis.

- **powersupply type**
  Configures the type of power supply that is connected to the chassis.

MIB Objects

  N/A
show fan

Displays the current operating status of chassis fans.

show fan [slot]

---

**Syntax Definitions**

*slot* 
Specifies the slot number of the fantray.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360 6465 6560 6570M 6860 6860N 6865 6900 6900 V72/C32 6900 X48C6/T48C6/ X48C4E/V48C8/ C32E/T24C2 X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guideline**

N/A

---

**Examples**

```
-> show fan
Chassis Fan Status
------------------------
 1 1 Running
 1 2 Running
 1 3 Running
 1 4 Not Running
```

**output definitions**

<table>
<thead>
<tr>
<th>Chassis/Tray</th>
<th>The chassis/tray ID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fan</td>
<td>The fan number describing the fan position.</td>
</tr>
<tr>
<td>Status/Functional</td>
<td>The current operational status of the corresponding fan.</td>
</tr>
<tr>
<td>Speed</td>
<td>The speed of the fan.</td>
</tr>
<tr>
<td>Airflow</td>
<td>-</td>
</tr>
</tbody>
</table>

---

**Release History**

Release 7.1.1; command introduced.
Related Commands

**show fan**

Displays the current operating status of chassis fantrays.

MIB Objects

N/A
**show fantray**

Displays the current operating status of chassis fantrays.

**show fantray [slot]**

---

### Syntax Definitions

| slot | Specifies the slot number of the fantray. |

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guideline

N/A

### Examples

```
-> show fantray
 | Working | Fan |
Tray | Status | Fans | Load % |
-----|--------|------|--------|
1     ON      4        50
```

### output definitions

| Chassis/Tray | The chassis/Tray ID. |
| Status       | The current operational status of the fantray. |
| Working Fans | The number of working fans. |
| Fan Load %   | The load of the fantray. |

### Release History

Release 7.1.1; command introduced.
Related Commands

**show fantray**
Displays the current operating status of chassis fantrays.

MIB Objects

N/A
show temperature

Displays the internal operating temperature of the chassis, as well as current temperature threshold settings.


Syntax Definitions

index Specifies the index number.
cmm_letter Specifies the CMM letter.
chassis The ID number of the chassis.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command displays the internal operating temperature, not the ambient temperature, of the current operating chassis as well as current temperature threshold settings.
- Refer to the appropriate Hardware Users Guide for detailed information about temperature thresholds for a specific OmniSwitch model.

Examples

-> show temperature
Chassis/Device | Current | Range | Danger | Thresh | Status
-----------------------------------------------
1/CMMA        | 48     | -45 to 93 | 98    | 93    | UNDER THRESHOLD

output definitions

Chassis/Device The device being measured (CMM, Fabric, or NI)
Current The current CPU temperature in Celsius.
Range The supported threshold range.
Danger The danger threshold value. This value is based on the switch model and is not configurable.
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thresh</td>
<td>The warning temperature threshold, in degrees Celsius. If the switch reaches or exceeds this temperature, the primary switch or CMM TEMP LED displays amber and a warning is sent to the user.</td>
</tr>
<tr>
<td>Status</td>
<td>Whether the current temperature has reached the threshold.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command introduced.

Related Commands

show fan

Displays the hardware information and current status for the chassis fans.

MIB Objects

chasChassisTable
  - chasHardwareBoardTemp
  - chasHardwareCpuTemp
  - chasTempRange
  - chasTempThreshold
  - chasDangerTempThreshold
show hash-control

Displays the current hash control settings for the switch.

show hash-control [non-ucast]

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show hash-control
Hash Mode   = brief,
Udp-Tcp-Port = disabled

-> show hash-control non-ucast
Hash Status = Enabled,
Hash Mode   : Normal

output definitions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash Mode</td>
<td>The current Hash Mode.</td>
</tr>
<tr>
<td>Udp-Tcp-Port</td>
<td>Status of UDP/TCP hashing.</td>
</tr>
<tr>
<td>Non-ucast Hash Status</td>
<td>Status of Non-ucast Hash status.</td>
</tr>
</tbody>
</table>

Release History

Release 7.2.1; command introduced.
Related Commands

powersupply type

Configures the hash mode of the switch.

MIB Objects

alaChasHashMode
alaChasUdpTcpPortMode
alaChasNonUCHashControl
show license-info

Displays all the licensed applications installed on the switch.

show license-info

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to verify which licenses are installed on the switch.
- The number of days remaining is only applicable for demo licenses.
- The module type will continue to display as ‘U16L’ even after upgrading a ‘U16’ to a ‘U16E’.

**Examples**

-> show license-info

<table>
<thead>
<tr>
<th>VID</th>
<th>device</th>
<th>license</th>
<th>type</th>
<th>Time (Days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>AV</td>
<td>permanent</td>
<td>NA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>DC</td>
<td>permanent</td>
<td>NA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>10G</td>
<td>permanent</td>
<td>NA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>MACSE</td>
<td>permanent</td>
<td>NA</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>METRO</td>
<td>permanent</td>
<td>NA</td>
</tr>
</tbody>
</table>

**output definitions**

- **VID**: Virtual chassis identifier.
- **Device**: Slot number of NI.
- **License**: Displays the feature license installed on the switch.
- **Type**: The type of license.
**Release History**

Release 7.2.1; command was introduced.
Release 8.6R1; **Upgrade Status** and **Expiration Date** fields added.
Release 8.9R1; **Upgrade Status** and **Expiration Date** fields removed.

**Related Commands**

- **license apply file**
  Activates the license for licensed protocols on the switch.

**MIB Objects**

- alaVcCapManSwLicensingInfoTable
  - alaVcLicensedvcSlot
  - alaVcLicensedMask
  - alaVcLicenseType
  - alaVcTimeRemain

**output definitions**

<table>
<thead>
<tr>
<th>VID</th>
<th>Virtual chassis identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Slot number of NI.</td>
</tr>
<tr>
<td>License</td>
<td>Displays the feature license installed on the switch.</td>
</tr>
<tr>
<td>Time (Days) Remaining</td>
<td>Time of days remaining for a demo license. Display as ‘NA’ for permanent licenses.</td>
</tr>
</tbody>
</table>
**show bluetooth status**

Displays the current USB adapter with Bluetooth technology configuration.

**show bluetooth status**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guideline**

N/A

**Examples**

```bash
-> show bluetooth status
Admin Status   : disabled,
Transmit Power : low,

Chassis Operational Status
---------------------------
1               Not Present
```

**output definitions**

- **Admin Status**: Whether the USB adapter with Bluetooth technology is enabled or disabled.
- **Transmit Power**: Whether transmit power is high or low.
- **Chassis**: The chassis identifier.
- **Operational Status**:
  - `notPresent`—No USB adapter with Bluetooth technology present.
  - `connectionInactive`—USB adapter with Bluetooth technology present but inactive.
  - `connectionActive`—USB adapter with Bluetooth technology present and active.
**Release History**

Release 8.1.1; command introduced.

**Related Commands**

- **bluetooth**

  Enables or disables a USB adapter with Bluetooth technology and configures the power level.

**MIB Objects**

| N/A |
**show me**

Executes an LED blink pattern for 10 seconds that is used by the USB adapter with Bluetooth technology to identify the connected switch.

**show me**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guideline**

Use this command in a virtual chassis to identify which switch currently has USB adapter with Bluetooth technology connectivity.

**Examples**

```
-> show me
The Chassis ID LED will blink for 10 seconds.
```

**Release History**

Release 8.1.1; command introduced.

**Related Commands**

- **bluetooth**: Enables or disables a USB adapter with Bluetooth technology and configures the power level.

**MIB Objects**

N/A
**show tcam utilization**

Displays runtime information about the Ternary Content Addressable Memory (TCAM) utilization for each stage of each TCAM on each slot of the switch.

```
show tcam utilization [chassis/slot] [chassis/slot/tcam]
```

**Syntax Definitions**

- `chassis/slot`: A chassis ID and slot number. Use this parameter to display TCAM utilization for a specific slot.
- `chassis/slot/tcam`: A chassis ID, slot, and TCAM number. Use this parameter to display utilization for a specific TCAM.

**Defaults**

By default, TCAM utilization is displayed for the entire switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The utilization is represented in terms of the minimum-sized entry supported by the TCAM.
- On an OmniSwitch 6860N, utilization statistics for the EM stage will display if the resource is configured. If the resource is not configured, all statistics for EM will show as zero. On the other OmniSwitch platforms, EM statistics will always show as zero.
- This command replaces the `show qos slice` command on the supported OmniSwitch platforms listed above; the `show qos slice` command, however, is still available on the other OmniSwitch platforms.

**Examples**

```
-> show tcam utilization
```

Legend:

- `C/S/T` = Chassis/Slot/TCAM
- `PI` = Pre-Ingress
- `I` = Ingress
- `E` = Egress
- `EM` = ExactMatch

<table>
<thead>
<tr>
<th>C/S/T</th>
<th>Stage</th>
<th>entry-</th>
<th>min-key-</th>
<th>min-key-</th>
<th>Utilization</th>
</tr>
</thead>
</table>
show tcam utilization

<table>
<thead>
<tr>
<th>size</th>
<th>entries</th>
<th>entries</th>
<th>percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>PI</td>
<td>10</td>
<td>236</td>
</tr>
<tr>
<td>1/1/1</td>
<td>I</td>
<td>10</td>
<td>333</td>
</tr>
<tr>
<td>1/1/1</td>
<td>E</td>
<td>10</td>
<td>24</td>
</tr>
<tr>
<td>1/1/1</td>
<td>EM</td>
<td>10</td>
<td>0</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.3.1; command introduced.
Release 8.7R2; EM stage added.

**Related Commands**

- `show tcam utilization detail` Displays additional TCAM usage information, such as application usage.

**MIB Objects**

- `alaTcamUtilTable`
- `alaTcamChassis`
- `alaTcamSlot`
- `alaTcamIndex`
- `alaTcamStage`
- `alaTcamEntrySize`
- `alaTcamUsedEntries`
- `alaTcamTotalEntries`
- `alaTcamPercentUsed`
show tcam utilization detail

Displays the Ternary Content Addressable Memory (TCAM) utilization of each application (or application group) for each stage of each TCAM on each slot of the switch.

show tcam utilization [chassis/slot] [chassis/slot/tcam] detail

Syntax Definitions

chassis/slot
A chassis ID and slot number. Use this parameter to display TCAM utilization for a specific slot.

chassis/slot/tcam
A chassis ID, slot, and TCAM number. Use this parameter to display utilization for a specific TCAM.

Defaults

By default, the detailed TCAM utilization is displayed for the entire switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The utilization is represented in terms of the minimum-sized entry supported by the TCAM.

Examples

-> show tcam utilization detail

Legend:
C/S/T = Chassis/Slot/TCAM
PI = Pre-Ingress
I = Ingress
E = Egress

<table>
<thead>
<tr>
<th>C/S/T</th>
<th>App Group</th>
<th>App Name</th>
<th>Resource Name</th>
<th>Stage</th>
<th>Entry</th>
<th>Used</th>
<th>Reserved</th>
<th>Available</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/1</td>
<td>SYSPRE</td>
<td>-</td>
<td>System PreIngress</td>
<td>PI 30</td>
<td>48</td>
<td>256</td>
<td>208</td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>TTI</td>
<td>-</td>
<td>System TTI</td>
<td>PI 30</td>
<td>0</td>
<td>2048</td>
<td>2048</td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>TUNNEL_SVC</td>
<td>-</td>
<td>Tunnel Services PreIngress</td>
<td>PI 30</td>
<td>0</td>
<td>512</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>SYSHI</td>
<td>-</td>
<td>System High</td>
<td>I 30</td>
<td>134</td>
<td>256</td>
<td>122</td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>SYSLO</td>
<td>-</td>
<td>System Low</td>
<td>I 60</td>
<td>76</td>
<td>256</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>TUNNEL_SVC</td>
<td>-</td>
<td>Tunnel Services Ingress</td>
<td>I 10</td>
<td>0</td>
<td>2052</td>
<td>2052</td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>QOS</td>
<td>-</td>
<td>QOS</td>
<td>I 60</td>
<td>0</td>
<td>512</td>
<td>512</td>
<td></td>
</tr>
<tr>
<td>1/1/1</td>
<td>UDPRLY</td>
<td>UDP_RLY_ISF</td>
<td>UDP_RLY_ISF</td>
<td>I 60</td>
<td>0</td>
<td>256</td>
<td>256</td>
<td></td>
</tr>
</tbody>
</table>
Chassis Management and Monitoring Commands

-> show tcam utilization 1/4/1 detail

Legend:
C/S/T = Chassis/Slot/TCAM
PI = Pre-Ingress
I = Ingress
E = Egress

<table>
<thead>
<tr>
<th>C/S/T</th>
<th>App Group</th>
<th>App Name</th>
<th>Resource Name</th>
<th>Stage</th>
<th>Entry Size</th>
<th>Used Entries</th>
<th>Reserved Entries</th>
<th>Available Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/4/1</td>
<td>SYSPRE</td>
<td>-</td>
<td>System PreIngress</td>
<td>PI</td>
<td>30</td>
<td>256</td>
<td>208</td>
<td></td>
</tr>
<tr>
<td>1/4/1</td>
<td>TTI</td>
<td>-</td>
<td>System TTI</td>
<td>PI</td>
<td>30</td>
<td>0</td>
<td>2048</td>
<td>2048</td>
</tr>
<tr>
<td>1/4/1</td>
<td>TUNNEL_SVC</td>
<td>-</td>
<td>Tunnel Services PreIngress</td>
<td>PI</td>
<td>30</td>
<td>0</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>1/4/1</td>
<td>SYSHI</td>
<td>-</td>
<td>System High</td>
<td>I</td>
<td>60</td>
<td>134</td>
<td>256</td>
<td>122</td>
</tr>
<tr>
<td>1/4/1</td>
<td>SYSLO</td>
<td>-</td>
<td>System Low</td>
<td>I</td>
<td>10</td>
<td>76</td>
<td>256</td>
<td>180</td>
</tr>
<tr>
<td>1/4/1</td>
<td>TUNNEL_SVC</td>
<td>-</td>
<td>Tunnel Services Ingress</td>
<td>I</td>
<td>10</td>
<td>0</td>
<td>2052</td>
<td>2052</td>
</tr>
<tr>
<td>1/4/1</td>
<td>-</td>
<td>QOS</td>
<td></td>
<td>I</td>
<td>120</td>
<td>0</td>
<td>512</td>
<td>512</td>
</tr>
<tr>
<td>1/4/1</td>
<td>-</td>
<td>UDPRLY UDP_RLY_ISF</td>
<td></td>
<td>I</td>
<td>120</td>
<td>0</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>1/4/1</td>
<td>-</td>
<td>ETHOAM</td>
<td></td>
<td>I</td>
<td>30</td>
<td>0</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td>1/4/1</td>
<td>-</td>
<td>PVLAN PVLAN1</td>
<td></td>
<td>I</td>
<td>60</td>
<td>0</td>
<td>256</td>
<td>256</td>
</tr>
<tr>
<td>1/4/1</td>
<td>-</td>
<td>PVLAN PVLAN2</td>
<td></td>
<td>E</td>
<td>30</td>
<td>0</td>
<td>256</td>
<td>256</td>
</tr>
</tbody>
</table>

Release History

Release 8.3.1; command introduced.

Related Commands

show tcam utilization
Displays runtime information about the TCAM utilization.

show tcam app-groups
Displays the application groups and the applications that belong to each group within the context of TCAM utilization.
MIB Objects

alaTcamDetailedUtilTable
alaTcamDTableChassis
alaTcamDTableSlot
alaTcamDTableTCAMIndex
alaTcamDTableStage
alaTcamDTableGResourceId
alaTcamDTableEntrySize
alaTcamDTableUsedEntries
alaTcamDTableReservedEntries
alaTcamDTableAvailableEntries
alaTcamDTableAppGroupName
alaTcamDTableAppName
alaTcamDTableResourceName
show tcam app-groups

Displays the application groups and the applications that belong to each group within the context of Ternary Content Addressable Memory (TCAM) utilization.

show tcam app-groups

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show tcam app-groups

App-Group Name                         App Name
---------------------------------------------------------------
SYSPRE                                 -
SYSHI                                  -
SYSLO                                  -
TTI                                    -
TUNNEL_SVC                             -
TUNNEL_SVC                             -
SYSEGR                                 -
EGR_SVC_PORT                           -
  - IPV6                                 -
  - QOS                                  -
  - PVLAN                                -
  - PVLAN                                -
  - AG                                   -

Release History

Release 8.3.1; command introduced.
Related Commands

- **show tcam utilization detail**  Displays additional TCAM usage information, such as application usage.
- **show tcam utilization**  Displays runtime information about the TCAM utilization.

MIB Objects

- alaTcamDetailedUtilTable
- alaTcamDTableChassis
- alaTcamDTableSlot
- alaTcamDTableTCAMIndex
- alaTcamDTableAppGroupName
- alaTcamDTableAppName
show capability profile

Displays the active and configured profile settings.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>X72</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The switch must be rebooted for the configured profile to take effect.
- On the OmniSwitch 6900-V72/C32, and OmniSwitch 6900-X72, this command displays the configured and active mode to indicate if the switch is operating in the router or switch mode. The configured mode is changed using the `capability profile` command.
- On the OmniSwitch 6560 and OmniSwitch 6570M, this command displays the configured and active TCAM mode (source or destination IPv6 filtering). The configured TCAM mode is changed using the `capability profile tcam mode` command.

Examples

Sample output on the OmniSwitch 6900-V72/C32, and OmniSwitch 6900-X72:

```
-> show capability profile
Configured Profile : Router
Active Profile     : Switch
```

Sample output on the OmniSwitch 6560:

```
-> show capability profile
Configured TCAM Mode : dest-ipv6
Active TCAM mode     : dest-ipv6
```

Release History

Release 8.5R2; command introduced.
Release 8.6R1; TCAM mode display added.
Related Commands

- **capability profile** Configures the mode of the switch to be either switch or router.
- **capability profile tcam mode** Configures the source IPv6 filtering or destination IPv6 filtering TCAM mode for the switch.

MIB Objects

alaCapManProfile
  - alaCapManProfileMode
alaCapManProfile
  - alaCapManProfileTcamMode
**show pmd-files**

Displays a list of PMD files generated on the switch.

show pmd-files

---

**Syntax Definitions**

N/A

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C4E/V48C8/C32E/T24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

-> show pmd-files

######################## PMD files(Chassis 1 /flash/pmd) ####################

pmd-capmanc-06.10.2014-15.24.49
pmd-agCmm-01.21.2016-15.07.32
pmd-agCmm-01.21.2016-15.08.09
pmd-capmanc-07.23.2016-14.28.25
pmd-capmanc-2016.07.23-14.42.42p
pmd-bcd2-07.13.2017-11.22.28

8 PMD files found

---

**Release History**

Release 8.4.1.R03; command introduced.
Related Commands

**show chassis**
Displays the basic configuration and status information for the switch chassis.

MIB Objects

N/A
show capability trap-threshold

Displays the capability trap-threshold configured values.

show capability trap-threshold

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the configured High and Low trap-threshold table utilization values.

**Examples**

```
-> show capability trap-threshold
Name       High    Low
----------+------+-------
MAC           95     90
ARP           95     90
```

**Release History**

Release 8.6R1; command introduced.

**Related Commands**

- `capability trap-threshold` Configures the MAC and ARP table utilization high and low values for generating the associated traps.

**MIB Objects**

- `alaCapManTrapThreshold`
  - `alaCapManTrapThresholdMacLow`
  - `alaCapManTrapThresholdMacHigh`
  - `alaCapManTrapThresholdArpLow`
alaCapManTrapThresholdArpHigh
show tech-support

Creates a log or tar file gathering important switch information that can be used by technical support.

show tech-support [layer2 | layer3 | eng [complete]]

Syntax Definitions

layer2 Gathers layer 2 switch configuration information.
layer3 Gathers layer 3 switch configuration information.
eng [complete] Gathers all relevant switch information from flash such as log files, configuration files, directories and creates an archive file with all the information.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Running the command with no parameters creates a tech_support.log file.
- The layer2 parameter creates a tech_support_layer2.log file.
- The layer3 parameter creates a tech_support_layer3.log file.
- The eng parameter creates a tech_support_eng.log file. The complete parameter creates a tech_support_complete.tar file with information from all switches in a VC along with the log files.
- Files with the prefix "smemcap" may be generated when the switch is operating at high memory usage. Ten files are generated before the switch reboots due to being out of memory. These files are cleared when the show tech-support eng complete command is run.

Examples

- show tech-support
- show tech-support layer2
- show tech-support layer3
- show tech-support eng
- show tech-support eng complete
Release History
Release 7.3.4.R02; command introduced.

Related Commands

**show chassis**
Displays the basic configuration and status information for the switch chassis.

MIB Objects

| N/A |
show mac-range

Displays the MAC range table.

show mac-range [index]

Syntax Definitions

index

Identifies the MAC range by referring to its position in the MAC range table.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The Chassis MAC Server (CMS) manages MAC addresses on the switch. The MAC addresses managed via the CMS are used as identifiers for the following functions:
  - Base chassis MAC address
  - Ethernet Management Port (EMP)
  - VLAN router ports
- Similar to IP addresses, MAC addresses are assigned by the Internet Assigned Numbers Authority (IANA) and distributed to users in sequential blocks. A sequential block of MAC addresses is referred to as a MAC address range.
- The MAC address range is stored on the switch’s EEPROM. The switch supports one MAC address range only. By default, this MAC address range contains thirty-two (32) factory-installed, contiguous MAC addresses.
- Because the switch currently supports one MAC address range only, index position 1 displays.

Examples

-> show mac range

<table>
<thead>
<tr>
<th>Mac Range</th>
<th>Row Status</th>
<th>Local/Global</th>
<th>Start Mac Addr</th>
<th>End Mac Addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>ACTIVE</td>
<td>GLOBAL</td>
<td>00:d0:95:6a:79:6e</td>
<td>00:d0:95:6a:79:8d</td>
</tr>
</tbody>
</table>
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Range</td>
<td>The MAC range index number (1). Because the switch currently supports one MAC address range only, index position 1 displays.</td>
</tr>
<tr>
<td>Row Status</td>
<td>The current status of the MAC range. The status <strong>ACTIVE</strong> refers to MAC addresses that are available for allocation to VLAN router ports and other applications.</td>
</tr>
<tr>
<td>Local/Global</td>
<td>The Local/Global status for MAC addresses in the range. Local MAC addresses have the local bit set in the first byte of the address. Global MAC addresses (also referred to as <strong>EEPROM</strong> MAC addresses) have the global bit set in the first byte of the address and are stored on the switch’s EEPROM. Because the switch’s default MAC range is stored on EEPROM, the status <strong>GLOBAL</strong> displays.</td>
</tr>
<tr>
<td>Start Mac Addr</td>
<td>The first MAC address in the MAC address range.</td>
</tr>
<tr>
<td>End Mac Addr</td>
<td>The last MAC address in the MAC address range.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

N/A

**MIB Objects**

- `chasMacAddressRangeTable`
  - `chasMacRangeIndex`
  - `chasGlobalLocal`
  - `chasMacAddressStart`
  - `chasMacAddressCount`
  - `chasMacRowStatus`
**show mac-range alloc**

Displays all allocated addresses from the MAC range table.

```
show mac-range [index] alloc
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>index</th>
<th>Identifies the MAC range by referring to its position in the MAC range table. Currently, index position 1 only is supported.</th>
</tr>
</thead>
</table>

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

N/A

**Examples**

```
-> show mac-range alloc
             Range    Mac Address         Application     Id
-----------------+-----------------+--------------------+---
01    00:d0:95:6b:09:40 CHASSIS              0
01    00:d0:95:6b:09:41 802.1X               0
01    00:d0:95:6b:09:5f CHASSIS              1
```

**output definitions**

<table>
<thead>
<tr>
<th>Range</th>
<th>The MAC range’s index number. The index number refers to the position of the range in the MAC range table. Values may range from 1–20. MAC ranges are divided by index number into four distinct categories. Refer to page 59-92 for more information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address</td>
<td>Current MAC address allocated for a specific application.</td>
</tr>
<tr>
<td>Application</td>
<td>The application for which the allocated MAC address is being used. Current options include VLAN, 802.1X, and CHASSIS. VLAN refers to MAC addresses allocated to VLAN router ports in multiple MAC router mode. CHASSIS refers to MAC addresses used for the base chassis MAC address and the Ethernet Management Port (EMP).</td>
</tr>
</tbody>
</table>
An ID number used to identify an allocated MAC address. ID numbers are used for the base chassis MAC address and Ethernet Management Port (EMP), as well as VLAN router ports. The ID value 0 is reserved for the switch's base chassis MAC address. The ID value 1 is reserved for the EMP MAC address. Router ports assigned to VLANs 2 through 4094 are given corresponding MAC IDs. For example, a router port configured on VLAN 44 receives an allocated MAC ID of 44. Because default VLAN 1 router ports use the base chassis MAC address by default, any router port configured on VLAN 1 is assigned the ID value 0.

Release History

Release 7.1.1; command introduced.

Related Commands

N/A

MIB Objects

ChasMacAddressAllocTable
  chasAppId
  chasObjectId
  chasAllocMacRangeIndex
  chasAllocMacAddress

output definitions (continued)
**show uboot config**

Displays the U-boot authentication status.

show uboot config

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

-> show uboot config
Uboot access: Disabled
Uboot authentication: Enabled

**Release History**

Release 8.7R3; command introduced

**Related Commands**

- **uboot access** Enables or disables the U-boot access.
- **uboot authentication** Enables or disables the U-boot authentication.

**MIB Objects**

- `alaAaaUbootAccess`
- `alaAaaUbootAuthenticationPassword`
**security key-chain gen-random-key**

Generates a 32-byte or 64-byte random key.

`security key-chain {gen-random-key | gen-random-key-256}`

### Syntax Definitions

- **gen-random-key**: Generates a 32-byte random key.
- **gen-random-key-256**: Generates a 64-byte random key.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The generated key can be used as an input value for hex-key or encrypt-key while creating a security key.

### Examples

```
-> security key-chain gen-random-key
0x0102030405060708090A0B0C0D0E0F

-> security key-chain gen-random-key-256
0x0102030405060708090A0B0C0D0E0F0102030405060708090A0B0C0D0E0F
```

### Release History

Release 8.4.1 R03; command introduced.
Release 8.7R1; **gen-random-key-256** keyword added.

### Related Commands

- **security key**: This command creates an authentication key into the system.

### MIB Objects

- N/A
security key

Creates an authentication key into the system.

security key key_id algorithm {simple | sha512 | sha384 | sha256 | sha224 | sha1 | md5} {encrypt-key encrypt_key | key simple_key} start-time mm/dd/yyyy [hh:mm] [lifetime days [hh:mm]]} {aes-gcm-256 | aes-gcm-128} {hex-key hex_key | encrypt-key {hex | num}} | {aes-cmac-256 | aes-cmac-128} {hex-key hex_key | encrypt-key {hex | num}}] keyed-name hex-kn}

no security key key_id [-key_id2]

Syntax Definitions

key_id The key ID. This can be in the range 1-256.
simple Specifies that the simple authentication algorithm is used as authentication key. This parameter is currently not supported.
sha512 Specifies that the SHA512 authentication algorithm is used as the authentication key. This parameter is currently not supported.
sha384 Specifies that the SHA384 authentication algorithm is used as the authentication key. This parameter is currently not supported.
sha256 Specifies that the SHA256 authentication algorithm is used as the authentication key.
sha224 Specifies that the SHA224 authentication algorithm is used as the authentication key. This parameter is currently not supported.
sha1 Specifies that the SHA1 authentication algorithm is used as the authentication key. This parameter is currently not supported.
md5 Specifies that the MD5 authentication algorithm is used as the authentication key. This parameter is currently not supported.
encrypt_key The key in hexadecimal format to provide security consideration on the authentication key. Configuration snapshot always displays authentication key in the encrypted form. The key can range from 16 to 512 characters in length.
simple_key Key will be plain text ASCII up to 118 characters. Use quotes (""") around the string if the key contains multiple words with spaces between them. Plain text key can range from 16 to 118 characters in length.
mm/dd/yyyy Key activation time. Granularity is up to minutes. Enter the start time in the format mm/dd/yyyy hh:mm where mm is the month, dd is the day, yyyy is the year, hh is the hour, mm is the minutes. For example, 08/08/2005 14:30
days Validity duration of the key in terms of days and time. Lifetime can be in the range 1 - 9125 days.
aes-gcm-256 Specifies that the AES-GCM-256 authentication algorithm is used as authentication key. This parameter is currently not supported.
aes-gcm-128 Specifies that the AES-GCM-128 authentication algorithm is used as authentication key.
aes-cmac-256 Specifies that the AES-CMAC-256 authentication algorithm is used as authentication key. This parameter is only supported on the OmniSwitch 6860N and OmniSwitch 6900-X48C4E.

aes-cmac-128 Specifies that the AES-CMAC-128 authentication algorithm is used as authentication key.

hex-key hex_key The key value in hexadecimal format (0xhex). Configuration snapshot displays the authentication key in the encrypted form. The key can range from 1 to 32 characters in length (16 byte) for AES-GCM-128 or AES-CMAC-128 algorithm, and 1 to 64 characters in length (32 byte) for AES-GCM-256 or AES-CMAC-256 algorithm.

encrpt-key hex The key in hexadecimal format. The key can range from 1 to 32 characters in length (16 byte) for AES-GCM-128 or AES-CMAC-128 algorithm, and 1 to 64 characters in length (32 byte) for AES-GCM-256 or AES-CMAC-256 algorithm.

encrpt-key num The key in numerical format. The key can range from 1 to 32 characters in length (16 byte) for AES-GCM-128 or AES-CMAC-128 algorithm, and 1 to 64 characters in length (32 byte) for AES-GCM-256 or AES-CMAC-256 algorithm.

hex-kn The Connectivity Association Key Name (CKN) value in hexadecimal format (0xhex). The key can range from 1 to 64 characters in length (32 byte) for AES-CMAC-128 algorithm, and 1 to 128 characters in length (64 byte) for AES-CMAC-256 algorithm.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>lifetime days</td>
<td>180 days</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The switch can have a maximum of 256 keys.
- Current active key is determined based on the lowest numerical key ID. When the current active key expires, if the keychain has multiple active keys, the switch will switchover to active key having lowest key ID.
- When the current active key expires, if the keychain does not have any other active key, the switch will bring down all the adjacencies formed using that keychain.
Parameters of a key can be modified if the key is not in use. Once the key is attached to any of the keychains, no more modification is allowed.

Use the `no` form of this command to delete a key.

To delete a key, first disassociate the keychain from a user application, and detach the key from the keychain.

The show commands will always display the key-string in an encrypted format.

Use the command `security key-chain gen-random-key` to generate a the hex-key to be configured for the AES-GCM-128 and AES-GCM-256 or AES-CMAC-128 and AES-CMAC-256 algorithm.

A keychain must have all keys of either 128-bit type or 256-bit type.

A keychain using the AES-GCM-128 authentication algorithm must be attached only to MACsec interface for its static-SAK configured under MACsec mode ‘static’. A keychain using the AES-CMAC-128 or AES-CMAC-256 authentication algorithm can be attached only to MACsec interface for its Static Connectivity Association Key (static-CAK) using Pre-Shared key configured under MACsec mode ‘dynamic’.

For more information on MACsec configuration, refer to the “Ethernet Port Commands” chapter in this guide.

**Examples**

```bash
-> security key 5 algorithm sha256 key "passwordstring123" start-time 1/31/2017 00:00 life-time 180 10:30
-> security key 5 algorithm sha256 key "passwordstring123" start-time 5/2/2017 life-time 150
-> security key 1 algorithm aes-gcm-128 hex-key 0x0102030405060708090A0B0C0D0E0F
-> security key 1 algorithm aes-cmac-128 hex-key 0x0102030405060708090A0B0C0D0E0F
  keyed-name 0x0102030405060708090A0B0C0D0FFF

-> no security key 5
```

**Release History**

Release 8.4.1; command introduced.
Release 8.4.1 R03; `aes-gcm-128` keyword added.
Release 8.5R2; `aes-cmac-128` keyword added.
Release 8.7R1; `aes-gcm-256` and `aes-cmac-256` keyword added.

**Related Commands**

- `show security key`  
  This command displays the configured keys in the system.

**MIB Objects**

- `alaSecKeyId`  
- `alaSecKeyAlgorithm`  
- `alaSecKeyType`  
- `alaSecKeyAuthKey`  
- `alaSecKeyStartTime`  
- `alaSecKeyLifeTime`  
- `alaSecKeyRowStatus`
security key-chain

This command creates a system level security keychain.

```
security key-chain key_chain_id [name key_chain_name]
```

```
no security key-chain key_chain_id1 [-key_chain_id2]
```

## Syntax Definitions

- `key_chain_id`: The keychain ID. This can be in the range 1-32.
- `key_chain_name`: The keychain name. The keychain name can range from 1 to 16 characters in length.

## Defaults

N/A

## Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Usage Guidelines

- There can be a maximum of 32 keychains in the device, and each of them can hold multiple keys of the same algorithm type.
- Use the `no` form of this command to delete a keychain.
- To delete a keychain, first disassociate the keychain from the user application.
- Deleting a keychain will not delete the keys associated with the keychain. Keys will subsequently remain configured, but will not be associated to any keychain, until reassociation.
- The keychain ID is associated to user applications such as ISIS, OSPF. The authentication information is carried in the Hello packet. If the authentication succeeds, then adjacency is formed. The two remote machines should have same current key ID, key and same authentication type.
- Changing the switch system clock impacts the status of the keys.

## Examples

```
-> security key-chain 1 globalKeyChain
-> no security key-chain 1-3
-> no security key-chain 4
```
Release History

Release 8.4.1; command introduced.

Related Commands

show security key-chain  This command displays the configured keychains in the system.

MIB Objects

alaSecKeyChainId
alasecKeyChainName
security key-chain key

This command associates a key into the specified keychain.

```
security key-chain key_chain_id key key_id [-key_id2]
no security key-chain key_chain_id1 [-key_chain_id1]
```

**Syntax Definitions**

- `key_chain_id` The keychain ID.
- `key_id` The key ID.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- A keychain can be configured with multiple keys of the same algorithm type.
- Use the `no` form of this command to disassociate a key from a security keychain.
- To disassociate a key from the keychain, first disassociate the keychain from the user application, and detach the key from the keychain.

**Examples**

```
-> security key-chain 1 key 5
-> no security key-chain 1
```

**Release History**

Release 8.4.1; command introduced.
Related Commands

- **security key-chain**
  This command creates a system level security keychain.

- **security key**
  This command creates an authentication key into the system.

- **show security key-chain**
  This command displays the configured keychains in the system.

MIB Objects

- alaSecKeyChainMappingKeyChainId
- alaSecKeyChainMappingKeyId
- alaSecKeyChainMappingRowStatus
**show security key**

This command displays the configured keys in the system.

```plaintext
show security key [key_id [-key_id2]]
```

### Syntax Definitions

- `key_id` - The key ID.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If key ID is not provided, information of all the keys is displayed.

### Examples

```
-> show security key
```

<table>
<thead>
<tr>
<th>ID</th>
<th>Status</th>
<th>Algorithm</th>
<th>Start-time</th>
<th>Life-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>expired</td>
<td>sha256</td>
<td>01/31/2016 10:30</td>
<td>100 00:00</td>
</tr>
<tr>
<td>2</td>
<td>valid</td>
<td>sha256</td>
<td>01/31/2016</td>
<td>1000 00:15</td>
</tr>
<tr>
<td>10</td>
<td>future</td>
<td>sha256</td>
<td>01/31/2017</td>
<td>180 (default)</td>
</tr>
<tr>
<td>24</td>
<td>valid</td>
<td>sha256</td>
<td>01/31/2016 05:00</td>
<td>0 12:20</td>
</tr>
</tbody>
</table>

**output definitions**

- **ID** - The key ID.
- **Status** - The status of the key.
- **Start-time** - Key activation time.
- **Life-time** - Validity duration of the key in terms of days and time.

### Release History

Release 8.4.1; command introduced.
Related Commands

**security key**

This command creates an authentication key into the system.

MIB Objects

- alasecKeychainId
- alasecKeyId
show security key-chain

This command displays the configured keychains in the system.

`show security key-chain [key_chain_id]`

### Syntax Definitions

- `key_chain_id`:
  The keychain ID.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6900V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If keychain ID is not provided, information of all the keychains is displayed.

### Examples

```
-> show security key-chain
ID   Name             current      Associated           User
     key          keys              applications
----+-------------------+--------+-------------------+-------------------------
1    globalKeychain         5          1,3,5-8,10      isis,isis_abc,ospf
2    vlan10Keychain        22         20,22           isis_123
```

### output definitions

- **ID**: The keychain ID.
- **Name**: The keychain name.
- **Current Key**: The current active key.
- **Associated Keys**: The keys associated with the keychain.
- **User Applications**: The keychain associated with the user application.

### Release History

Release 8.4.1; command introduced.
Related Commands

security key-chain
This command creates a system level security keychain.

security key-chain key
This command associates a key into the specified keychain.

MIB Objects

alaSecKeyChainId
alasecKeychainName
alarm in

Configures an alarm input. For an alarm input, action can be configured to either send an SNMP trap, log a SWLog message locally, or set alarm output.

alarm in alr_in_name [chassis-in chassis_id_in] action {swlog | trap | alarm-out} [admin-state {enable | disable}]

no alarm alr_in_name

Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alr_in_name</td>
<td>Name of the alarm input (1 to 32 characters).</td>
</tr>
<tr>
<td>chassis_id_in</td>
<td>Chassis identifier where alarm input is connected.</td>
</tr>
<tr>
<td>swlog</td>
<td>trap</td>
</tr>
<tr>
<td>enable</td>
<td>Enable the alarm input.</td>
</tr>
<tr>
<td>disable</td>
<td>Disable the alarm input.</td>
</tr>
</tbody>
</table>

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>disabled</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- By default, alarm is disabled for all actions.
- If the chassis ID is not configured, by default, local chassis is considered for the alarm input.
- Use the no form of this command to remove the alarm input.
- OmniSwitch 6465 switch has a single alarm input.
- The alarm status and alarm output will be updated to reflect a change in the alarm input.
- On reload of the switch, the alarm status and output alarm is set based on the current alarm input.

Examples

- `-> alarm in "temperature-sensor" action alarm-out`
-> alarm in "door-sensor" chassis-in 1 action alarm-out admin-state enable
-> alarm in "smoke-sensor" chassis-in 2 action trap swlog alarm-out admin-state enable

-> no alarm temperature-sensor

**Release History**

Release 8.5 R1; command introduced.

**Related Commands**

- **alarm clear status**
  
  Clears the status of the specified alarm.

- **show alarm input config**
  
  Displays the alarm input configuration.

- **show alarm status**
  
  Displays all the traps, system events, or alarm input for which the alarm output is raised.

**MIB Objects**

alaAlarmInputConfigTable
  
  - alaAlarmInputConfigName
  - alaAlarmInputConfigChassis
  - alaAlarmConfigInputTrapActionEnable
  - alaAlarmConfigInputSwlogActionEnable
  - alaAlarmConfigInputAlarmOutputActionEnable
  - alaAlarmConfigAdminStatus
  - alaAlarmInputConfigRowStatus
alarm event

Configures the listed system events or any trap for alarm output.

```
alarm event alr_event_name {event {vc-status-change | temperature | system-health | power-supply | port-violation network-port userport [-userport2] | port-health | link-down network-port userport [-userport2] | authentication-failure} | trapid id} [chassis-in chassis_id_in] [admin-state {enable | disable}]
```

no alarm alr_event_name

---

**Syntax Definitions**

- `alr_event_name`: Name of the alarm event or trap (1 to 32 characters).
- `userport`: Network port of the switch.
- `id`: Trap ID.
- `chassis_id_in`: Chassis identifier where alarm input is connected.
- `enable`: Enable the alarm event.
- `disable`: Disable the alarm event.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enable</code></td>
<td><code>disable</code></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- By default, alarm output action is disabled for all the alarm events.
- System events corresponds to critical failures of the switch. Alarm event can be configured for any of these supported system events.
- Trap ID corresponds to the SNMP traps supported in the switch. Use `show snmp-trap config` command to view the supported traps. Alarm event can be configured for any of these supported traps.
- Both event as well as trap cannot be configured for the same alarm event. If configured, the later is ignored with an error message.
Alarm event of the single chassis can be mapped to multiple alarm outputs on different chassis for redundancy.

Alarm events from multiple chassis can be mapped to alarm output on the single chassis.

Same network port can be configured for both link down as well as port violation event but with a different event name.

A network port that falls in the network port range, which is already configured to an event cannot be configured to another event.

If the chassis ID is not configured, by default, local chassis is considered for the alarm event.

Use the `no` form of this command to remove the alarm event.

**Examples**

```plaintext
-> alarm event system-fail event system-health
-> alarm event link-failure-critical event link-Down network-port 10-15 chassis-in
l admin-state enable

-> no alarm system-fail
```

**Release History**

Release 8.5 R1; command introduced.

**Related Commands**

- **alarm clear status**
  Clears the status of the specified alarm.

- **show alarm event config**
  Displays the alarm system event configuration.

- **show alarm status**
  Displays all the traps, system events, or alarm input for which the alarm output is raised.

**MIB Objects**

- `alarmEventConfigTable`
- `alarmEventConfigTable`
- `alarmEventConfigName`
- `alarmEventConfigEvent`
- `alarmEventConfigTrapId`
- `alarmEventConfigNetworkPortStart`
- `alarmEventConfigNetworkPortEnd`
- `alarmEventConfigInputChassis`
- `alarmEventConfigAdminStatus`
- `alaAlarmEventConfigRowStatus`
alarm out

Configures the alarm output relay of a chassis.

```
alarm out alr_out_name [chassis-out chassis_id_out] [admin-state {enable | disable}]
no alarm out alr_out_name
```

**Syntax Definitions**

- `alr_out_name`: Name of the alarm output (1 to 32 characters).
- `chassis_id_out`: Chassis identifier where alarm output is connected.
- `enable`: Enable the alarm output.
- `disable`: Disable the alarm output.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the chassis ID is not configured, by default, local chassis is considered for the alarm output.
- Use the `no` form of this command to remove the alarm output.
- OmniSwitch 6465 switch has single alarm output.

**Examples**

```
-> alarm out "critical-fault-detector"
-> alarm out "minor-fault-detector" chassis-out 2 action admin-state enable
-> alarm out "critical-fault-detector"
```

**Release History**

Release 8.5 R1; command introduced.
**Related Commands**

**show alarm status**
Displays all the traps, system events, or alarm input for which the alarm output is raised.

**MIB Objects**

alaAlarmOutputConfigTable
alaAlarmOutputConfigName
alaAlarmOutputConfigChassis
alaAlarmOutputConfigRowStatus
alarm map

Maps an alarm input or event with an alarm output within a chassis or any other chassis in the VC.

**alarm map** *alarm_name* out *alr_out_name*

**no alarm map** *alarm_name*

---

**Syntax Definitions**

- **alarm_name**: Name of the alarm input or system event (1 to 32 characters).
- **alr_out_name**: Name of the alarm output (1 to 32 characters)

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Alarm input or event of the single chassis can be mapped to multiple alarm outputs on different chassis for redundancy.
- Alarm input or event from multiple chassis can be mapped to alarm output on the single chassis.
- Use the **no** form to unmap the alarm input from alarm output.

---

**Examples**

- `--> alarm map "temperature-sensor" out "critical-fault-detector"
- `--> no alarm map "temperature-sensor"

---

**Release History**

Release 8.5 R1; command introduced.
Related Commands

- **alarm in**: Configures an alarm input.
- **alarm event**: Configures the listed system events or any trap for alarm output.
- **alarm out**: Configures the alarm output relay of a chassis.
- **show alarm status**: Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

- **alaAlarmMappingConfigTable**
  - **alaAlarmInputConfigName**
  - **alaAlarmOutputConfigName**
  - **alaAlarmMappingConfigRowStatus**
alarm duration

Configure the duration of an alarm.

```
alarm duration [[hour] [min] | [default]]
```

**Syntax Definitions**

- **hour**: Duration of the alarm in hours.
- **min**: Duration of the alarm in minutes.
- **default**: Sets the alarm duration to 24 hours 0 minutes.

**Defaults**

By default, the alarm duration is set to 24 hours 0 minutes.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- In a virtual chassis (VC) setup, alarm duration configuration applies to all the chassis of the VC.
- A minimum alarm duration of five minutes and a maximum alarm duration of 48 hours can be configured.
- An alarm is switched off for an input or event after the configured duration. If there are multiple events or input, alarm is switched off after the elapsed duration of all the events and input.
- Use `alarm clear status` command to force stop the alarm before the set alarm duration for any alarm event or input.
- Modification or updated duration is applied only to those alarms raised after the configuration change. Alarms which are in progress are not impacted.
- Use `default` option to reset the alarm duration to 24 hours 0 minutes.

**Examples**

- `-> alarm duration 2`
- `-> alarm duration default`

**Release History**

Release 8.5 R1; command introduced.
Related Commands

**alarm clear status**
Clears the status of the specified alarm.

**show alarm status**
Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

  - alarmDurationConfigHour
  - alarmDurationConfigMin
alarm clear status

Clears the status of the specified alarm.

`alarm clear status [alarm_name]`

**Syntax Definitions**

- `alarm_name`: Name of the alarm input or alarm event.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The command does not disable or remove the alarm.
- The command can be used to forcibly stop the alarm and clear the status.
- If the output alarm is ON for multiple events or input, all the alarms have to be cleared to switch off the alarm output.
- If the alarm name is not specified, all the configured alarms are cleared.

**Examples**

- `-> alarm clear status temperature-sensor`
- `-> alarm clear status`

**Release History**

Release 8.5 R1; command introduced.
Related Commands

show alarm status Displays all the traps, system events, or alarm input for which the alarm output is raised.

MIB Objects

alarmStatusTable
   alarmStatusInputName
   alarmStatusOutputName
   alarmStatusInputChassis
   alarmStatusOutputChassis
   alarmStatusTimeStamp
   alarmStatusTrapid
**show alarm input config**

Displays the alarm input configuration.

`show alarm input config chassis chassis_id`

---

**Syntax Definitions**

- `chassis_id`: Chassis identifier.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The command displays configuration of all the chassis if chassis ID is not specified.

**Examples**

`-> show alarm input config`

```
Alarm Duration 5 hrs 30 Mins
```

<table>
<thead>
<tr>
<th>Alarm-Name</th>
<th>Chassis-in</th>
<th>Action</th>
<th>Alarm-Output-Name</th>
<th>Chassis-out</th>
<th>Admin-State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature Sensor</td>
<td>1</td>
<td>Alarm-Output</td>
<td>critical-fault-detector</td>
<td>1</td>
<td>enable</td>
</tr>
<tr>
<td>fire Sensor</td>
<td>1</td>
<td>trap</td>
<td>N/A</td>
<td>N/A</td>
<td>enable</td>
</tr>
<tr>
<td>Temperature Sensor</td>
<td>1</td>
<td>Alarm-Output</td>
<td>minor-fault-detector</td>
<td>2</td>
<td>enable</td>
</tr>
<tr>
<td>door Sensor</td>
<td>1</td>
<td>Alarm-Output</td>
<td>minor-fault-detector</td>
<td>2</td>
<td>enable</td>
</tr>
</tbody>
</table>

**output definitions**

- **Alarm-Name**: Name of the alarm.
- **Chassis-in**: Chassis identifier where alarm input is connected.
- **Action**: The action sent on the alarm output.
- **Alarm-Output-Name**: Name of the alarm output.
- **Chassis-out**: Chassis identifier where alarm output is connected.
- **Admin-State**: Status of the alarm.
Release History

Release 8.5 R1; command introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alarm in</td>
<td>Configures an alarm input.</td>
</tr>
<tr>
<td>show alarm status</td>
<td>Displays all the traps, system events, or alarm input for which the alarm output is raised.</td>
</tr>
</tbody>
</table>

MIB Objects

alaAlarmInputConfigTable
  - alaAlarmInputConfigName
  - alaAlarmInputConfigChassis
  - alaAlarmConfigInputTrapActionEnable
  - alaAlarmConfigInputSwlogActionEnable
  - alaAlarmConfigInputAlarmOutputActionEnable
  - alaAlarmConfigAdminStatus
  - alaAlarmInputConfigRowStatus

alaAlarmInputConfigTable
  - alaAlarmOutputConfigName
  - alaAlarmOutputConfigChassis
  - alaAlarmOutputConfigRowStatus

alaAlarmMappingConfigTable
  - alaAlarmInputConfigName
  - alaAlarmOutputConfigName
  - alaAlarmMappingConfigRowStatus
show alarm event config

Displays the alarm system event configuration.

show alarm event config chassis chassis-id

Syntax Definitions

chassis_id  Chassis identifier.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>chassis-id</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- The command displays configuration of all the chassis if chassis ID is not specified.
- Network port is only applicable for link-down and port violation event.

Examples

-> show alarm event config

Alarm Duration 5 hrs 30 Mins

<table>
<thead>
<tr>
<th>Alarm-Name</th>
<th>Chassis-In</th>
<th>Network-Port</th>
<th>Trap-Id</th>
<th>Event-Name</th>
<th>Alarm-Output-Name</th>
<th>Chassis_out</th>
<th>Admin-State</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-fail</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>system-health</td>
<td>minor-fault-detector</td>
<td>2</td>
<td>enable</td>
</tr>
<tr>
<td>power-fail</td>
<td>1</td>
<td>N/A</td>
<td>N/A</td>
<td>power-supply</td>
<td>minor-fault-detector</td>
<td>2</td>
<td>enable</td>
</tr>
<tr>
<td>login-failure</td>
<td>2</td>
<td>N/A</td>
<td>5</td>
<td>N/A</td>
<td>minor-fault-detector</td>
<td>2</td>
<td>enable</td>
</tr>
</tbody>
</table>

output definitions

- **Alarm-Name**: Name of the alarm.
- **Chassis-in**: Chassis identifier where alarm input is connected.
- **Network-Port**: Network port of the chassis.
- **Trap-ID**: Trap ID.
- **Event-Name**: Name of the system event.
- **Alarm-Output-Name**: Name of the alarm output.
**output definitions**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Chassis-out</td>
<td>Chassis identifier where alarm output is connected.</td>
</tr>
<tr>
<td>Admin-State</td>
<td>Status of the alarm.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.5 R1; command introduced.

**Related Commands**

- **alarm event**
  Configures the listed system events or any trap for alarm output.

- **show alarm status**
  Displays all the traps, system events, or alarm input for which the alarm output is raised.

**MIB Objects**

```
alarmEventConfigTable
  alarmEventConfigName
  alarmEventConfigEvent
  alarmEventConfigTrapId
  alarmEventConfigNetworkPortStart
  alarmEventConfigNetworkPortEnd
  alarmEventConfigInputChassis
  alarmEventConfigAdminStatus
  alaAlarmEventConfigRowStatus

alaAlarmOutputConfigTable
  alaAlarmOutputConfigName
  alaAlarmOutputConfigChassis
  alaAlarmOutputConfigRowStatus

alaAlarmMappingConfigTable
  alaAlarmInputConfigName
  alaAlarmOutputConfigName
  alaAlarmMappingConfigRowStatus
```
show alarm status

Displays all the traps, system events, or alarm input for which the alarm output is raised. For a VC, the alarm status for each chassis is displayed.

show alarm status chassis chassis-id

Syntax Definitions

chassis_id

Chassis identifier.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Network port displays the status on the port range or a specific port.
- If the same failure (input or event or trap) is repeated, the data structure is updated with the latest failure.

Examples

-> show alarm status chassis-id 2

<table>
<thead>
<tr>
<th>Alarm-Name</th>
<th>Chassis-In</th>
<th>Time-Stamp</th>
<th>Network-Port</th>
<th>Trap-ID</th>
<th>Event-Name</th>
<th>Alarm-Output</th>
<th>Chassis-Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>login-failure</td>
<td>2</td>
<td>09/31/2017 : 14:30:00</td>
<td>N/A</td>
<td>5</td>
<td>N/A</td>
<td>minor-fault-detector</td>
<td>2</td>
</tr>
</tbody>
</table>

output definitions

- **Alarm-Name**: Name of the alarm.
- **Chassis-in**: Chassis identifier where alarm input is connected.
- **Time-Stamp**: The system time of the switch where the alarm occurred.
- **Network-Port**: Network port of the chassis.
- **Trap-ID**: Trap ID.
- **Event-Name**: Name of the system event.
- **Alarm-Output**: Name of the alarm output.
- **Chassis-out**: Chassis identifier where alarm output is connected.
Release History
Release 8.5 R1; command introduced.

Related Commands

- **show alarm input config** Displays the alarm input configuration.
- **show alarm event config** Displays the alarm system event configuration.

MIB Objects

- alarmStatusTable
  - alarmStatusInputName
  - alarmStatusOutputName
  - alarmStatusInputChassis
  - alarmStatusOutputChassis
  - alarmStatusTimeStamp
  - alarmStatusTrapid
  - alarmStatusEvent
  - alarmStatusNetworkPortStart
  - alarmStatusNetworkPortEnd
  - alarmStatusClear
appmgr

Configures the installed applications.

```
appmgr {start | stop | restart} |ams broker | config-sync | config-dbase | ams cron-app | [ams-apps
iot-profiler] | [aos-ovsdb ovsdb-app]
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>start</strong></td>
<td>Starts the specified application from package.</td>
</tr>
<tr>
<td><strong>stop</strong></td>
<td>Stops the specified application from package.</td>
</tr>
<tr>
<td><strong>restart</strong></td>
<td>Starts and stops the specified application from package.</td>
</tr>
<tr>
<td><strong>broker</strong></td>
<td>Broker instance of AMS</td>
</tr>
<tr>
<td><strong>config-sync</strong></td>
<td>An AMS component application which is used to synchronize the configuration in the network.</td>
</tr>
<tr>
<td><strong>config-dbase</strong></td>
<td>Another AMS component application that helps to store and replay the configuration to new nodes in the network.</td>
</tr>
<tr>
<td><strong>cron-app</strong></td>
<td>An application for running the scheduled time based jobs with AMS.</td>
</tr>
<tr>
<td><strong>iot-profiler</strong></td>
<td>An AMS-app application, responsible for sharing the IoT profiled data with OmniVista for the integrated IoT OV-Switch solution.</td>
</tr>
<tr>
<td><strong>aos-ovsdb ovsdb-app</strong></td>
<td>Configures the client and server for the OVSDB application.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Enter `appmgr` without any parameters to see the command syntax.
- The package manager and app manager commands can be run by administrators only with write privileges to the SYSTEM partition management family.

### Examples

```
-> appmgr start ams broker
-> appmgr start ams config-sync
-> appmgr start ams config-dbase
-> appmgr start ams cron-app argument "5 python3 /flash/python/hello.py , 1 python3
```
/flash/python/hello1.py
-> write memory
-> show appmgr
Legend: (+) indicates application is not saved across reboot

<table>
<thead>
<tr>
<th>Application</th>
<th>Status</th>
<th>Package Name</th>
<th>User</th>
<th>Status Time Stamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>broker</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Nov 26 13:28:27 2019</td>
</tr>
<tr>
<td>config-sync</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Nov 26 13:28:27 2019</td>
</tr>
<tr>
<td>config-dbase</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Nov 26 13:28:27 2019</td>
</tr>
<tr>
<td>iot-profiler</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Nov 26 13:28:27 2019</td>
</tr>
<tr>
<td>cron-app</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Mar 15 18:55:18 2021</td>
</tr>
</tbody>
</table>

-> appmgr start ams-apps iot-profiler -args -h 10.10.10.1 -p 1883
Success to start iot-profiler

**Release History**

Release 8.6R1; command introduced.
Release 8.6R2; command syntax and command output modified.
Release 8.7R3; **cron-app** support added.

**Related Commands**

- appmgr list
  Displays the application currently launched/stopped/committed.
- appmgr commit
  Use this command to save the configuration across reboots.
- show appmgr
  Displays the application currently started/stopped/committed.

**MIB Objects**

N/A
appmgr list

Displays the application currently started/stopped/committed.

appmgr list [app_name]

Syntax Definitions

app_name Specify the name of the application.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

Enter appmgr without any parameters to see the command syntax.

Examples

-> appmgr list
Legend: (+) indicates application is not saved across reboot
Application Status Package Name User Status TimeStamp
---------------------------------------------------------------------------------------------------------------------
+ broker stopped ams admin Mon Nov 25 17:07:54 2019
config-sync started ams admin Tue Nov 12 11:43:12 2019
config-dbase started ams admin Tue Nov 12 11:43:39 2019

-> appmgr list iot-profiler
Package Name          : ams-apps
Committed (Yes/No)    : No
Status                : started
Timestamp             : Apr 16, 2014: 02:20:02
User                  : admin
Command line arguments : -h 10.10.10.1 -p 1883
Installation script   : /flash/working/pkg/ams-apps/install.sh

output definitions

Application Displays the name of the Application.
Status Displays the status of the Application.
Package Name Displays the name of the package.
User Displays the user information.
Status TimeStamp Displays the timestamp status information.
Release History

Release 8.6R2; command introduced.
Release 8.7R2; command deprecated. Use `show appmgr`.

Related Commands

appmgr

Use this command to start the tasks for AOS Micro Services (AMS).

MIB Objects

N/A
show appmgr

Displays the application currently started/stopped/committed.

show appmgr

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Enter `show appmgr` without any parameters to see the overall information.
- Enter the application parameter to see the information specific to the application.

**Examples**

`-> show appmgr`

Legend: (+) indicates application is not saved across reboot

<table>
<thead>
<tr>
<th>Application</th>
<th>Status</th>
<th>Package Name</th>
<th>User</th>
<th>Status TimeStamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ broker</td>
<td>stopped</td>
<td>ams</td>
<td>admin</td>
<td>Mon Nov 25 17:07:54 2019</td>
</tr>
<tr>
<td>config-sync</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Nov 12 11:43:12 2019</td>
</tr>
<tr>
<td>config-dbase</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Nov 12 11:43:39 2019</td>
</tr>
<tr>
<td>cron-app</td>
<td>started</td>
<td>ams</td>
<td>admin</td>
<td>Tue Mar 15 18:55:18 2021</td>
</tr>
</tbody>
</table>

`-> show appmgr cron-app`

| Package Name            | : ams,                  |
| Committed (Yes/No)      | : No,                   |
| Status                  | : started,              |
| Timestamp               | : Tue Mar 15 18:55:18 2021, |
| User                    | : admin,                |
| Command line arguments  | : 5 python3 /flash/python/hello.py , 1 python3 /flash/python/ hello1.py, |
| Installation script     | : /flash/working/pkg/ams/install.sh |

**output definitions**

| Application          | Displays the name of the Application. |
| Status               | Displays the status of the Application. |
| Package Name         | Displays the name of the package. |

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 59-131
output definitions

<table>
<thead>
<tr>
<th>User</th>
<th>Displays the user information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status TimeStamp</td>
<td>Displays the timestamp status information.</td>
</tr>
</tbody>
</table>

Release History

Release 8.7R2; command introduced.

Related Commands

appmgr

Use this command to start the tasks for AOS Micro Services (AMS).

write memory

Copies the current configuration (RAM) to the RUNNING DIRECTORY on the primary CMM.

MIB Objects

N/A
appmgr commit

Saves the configuration across reboots.

appmgr commit

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

Enter `appmgr` without any parameters to see the command syntax.

**Examples**

`-> appmgr commit`

**Release History**

Release 8.6R2; command introduced.
Release 8.7R2; command deprecated. Use `write memory`.

**Related Commands**

appmgr

Use this command to start the tasks for AOS Micro Services (AMS).

**MIB Objects**

N/A
pkgmgr

Installs Debian packages for non-AOS software applications.

```
pkgmgr {[install | verify] package_file_name | remove package_name}
```

### Syntax Definitions

- **install**: Extracts and installs the contents of the package to system memory.
- **remove**: Removes all the files of this package from system memory.
- **verify**: Verifies the ALE signature and the checksums for the Debian package.

**package_file_name**: Name of the Debian package file

**package_name**: Name of the package displayed in output of `show pkgmgr` command.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The package manager and app manager commands can be run by administrators only with write privileges to the SYSTEM partition management family.

- The Debian package must be downloaded from the service and support website (`businessportal2.alcatel-lucent.com`).

- The Debian package file must be copied to the `pkg` in the running directory. For example, if working is the running directory, then copy to `/flash/working/pkg` directory of the switch.

- Use the `pkgmgr verify` command to verify the contents of the package. It also provides the version compatibility information for the release.

- Compatible release in the `pkgmgr verify` output displays the release which is compatible with the package. The "&gt;=" sign means the package is compatible for AOS release version greater than or equal to the version displayed in "Compatible release". If the sign is not displayed then it is compatible only for that release version only.

- Use the `pkgmgr install` command to install the package.
After the package is installed successfully, use the **write memory** command to save the installation permanently.

If the switch restricts installation of the package due to memory threshold, use the **health threshold memory** command to increase the RAM memory threshold of the switch.

Use the **pkgmgr remove** command to remove the package.

**Note.** In a Virtual Chassis environment, if this **pkgmgr** command is successful on Master unit, it will be automatically executed on all units of the Virtual Chassis.

**Examples**

```
-> pkgmgr verify uos-ams-apps-v1.deb
uos-ams-apps-v1.deb
Verifying MD5 checksum.. OK
Compatible release: >=8.7.3-0

-> pkgmgr install uosn-ams-apps-v1.deb
Verifying MD5 checksum.. OK
System Memory check.. PASS
Extracting control files for package uosn-ams-apps-v1.deb .. OK
TARGET_AOS_PLATFORMS
No requirement to check target platform
Package target platforms check.. PASS
Package Dependency check.. PASS
Preparing to replace ams-apps 1 (using /flash/working/pkg/uosn-ams-apps-v1.deb)...
Setting up ams-apps (1)... Installing package uosn-ams-apps-v1.deb .. OK
Write memory is required complete package ams-apps installation

-> write memory

-> pkgmgr remove ams
CLI output:
Purging ams-apps (1)... Removing package ams-apps.. OK
Write memory is required complete package ams-apps removal

-> pkgmgr verify package-webview-v1.deb
CLI output:
Verifying MD5 checksum.. OK
Compatible release: >= 8.7.3-0

-> pkgmgr install package-webview-v1.deb
Verifying MD5 checksum.. OK
System Memory check.. PASS
Extracting control files for package package-webview-v1.deb .. OK
TARGET_AOS_PLATFORMS
No requirement to check target platform
Package target platforms check.. PASS
Package Dependency check.. PASS
Unpacking webview (from /flash/working/pkg/package-webview-v1.deb)...
Setting up webview (1)...
Installing package package-webview-v1.deb .. OK
Write memory is required complete package webview installation

-> write memory

-> pkgmgr remove webview
CLI output:
Purging webview (1)...
Removing package webview.. OK
Write memory is required complete package webview removal

Release History
Release 8.6R2; command introduced.
Release 8.7R3; pkgmgr compatible release added.

Related Commands

- **show pkgmgr**
  Displays the packages currently installed/committed.

- **write memory**
  Use this command to save all ‘installed’ packages so that they can be restored after reboot.

MIB Objects

- N/A
**show pkgmgr**

Displays the packages currently installed/committed.

`show pkgmgr [package_name]`

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command replaces the `pkgmgr list` command which was deprecated in 8.7R2.

**Examples**

```
-> show pkgmgr ams
Package Name     : ams,
Committed (Yes/No): Yes,
Version          : default,
Filename          : uosn-ams-apps-v1.deb,
Status           : installed,
Timestamp        : ,
User              : root,
Installation script : default

-> show pkgmgr
Legend: (+) indicates package is not saved across reboot
(*) indicates packages will be installed or removed after reload

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Status</th>
<th>Install Script</th>
</tr>
</thead>
<tbody>
<tr>
<td>ams</td>
<td>1</td>
<td>installed</td>
<td>/flash/working/pkg/ams/install.sh</td>
</tr>
<tr>
<td>webview</td>
<td>1</td>
<td>installed</td>
<td>/flash/working/pkg/webview/install.sh</td>
</tr>
<tr>
<td>ams-apps</td>
<td>1</td>
<td>installed</td>
<td>/flash/working/pkg/ams-apps/install.sh</td>
</tr>
</tbody>
</table>
```
output definitions

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Displays the name of the package.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committed (Yes/No)</td>
<td>Displays whether the package is committed or not.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the version of the package.</td>
</tr>
<tr>
<td>Filename</td>
<td>Displays the filename.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the status of the package.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>Displays the timestamp.</td>
</tr>
<tr>
<td>User</td>
<td>Displays the name of user information.</td>
</tr>
<tr>
<td>Install Script</td>
<td>Displays the install script details.</td>
</tr>
</tbody>
</table>

Release History

Release 8.7R2; command introduced.

Related Commands

pkgmgr

Use this command to install the required non-AOS software applications (developed by ALE and/or ALE-approved partners) Debian package.

write memory

Use this command to save all ‘installed’ packages so that they can be restored after reboot.

MIB Objects

N/A
pkgmgr commit

Saves all ‘installed’ packages so that they can be restored after reboot.

pkgmgr commit

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

Not supported in this release.

**Usage Guidelines**

This command was deprecated in 8.7R2. Use the write memory command.

**Examples**

-> pkgmgr commit

**Release History**

Release 8.6R2; command introduced.
Release 8.7R2; command deprecated.

**Related Commands**

- **pkgmgr**
  
  Use this command to install the required non-AOS software applications (developed by ALE and/or ALE-approved partners) Debian package.

- **show pkgmgr**
  
  Displays the packages currently installed/committed.

**MIB Objects**

N/A
The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver. It provides client time accuracies within a millisecond on LANs, and up to a few tens of millisecond on WANs. Typical NTP configurations utilize multiple redundant servers and diverse network paths in order to achieve high accuracy and reliability.

It is important for networks to maintain accurate time synchronization between network nodes. The standard timescale used by most nations of the world is based on a combination of Universal Coordinated Time (UTC) (representing the Earth’s rotation about its axis) and the Gregorian Calendar (representing the Earth’s rotation about the Sun). UTC time is disseminated by various means, including radio and satellite navigation systems, telephone modems, and portable clocks.

The MIB information for NTP is as follows:

- **Filename:** ALCATEL-IND1-NTP-MIB.mib
- **Module:** alcatelIND1NTPMIB
A summary of available commands is listed here:

- ntp server
- ntp server synchronized
- ntp server unsynchronized
- ntp client
- ntp src-ip preferred
- ntp broadcast
- ntp broadcast-client
- ntp broadcast-delay
- ntp key
- ntp key load
- ntp authenticate
- ntp master
- ntp interface
- ntp max-associations
- ntp broadcast
- ntp peer
- ntp vrf-name
- show ntp status
- show ntp client
- show ntp client server-list
- show ntp server client-list
- show ntp server status
- show ntp keys
- show ntp peers
- show ntp server disabled-interfaces
**ntp server**

Specifies an NTP server from which the switch will receive updates.

```
ntp server {ip_address | server_name} [key key_id | | minpoll poll | maxpoll poll | version version | prefer | burst | iburst | preempt]
no ntp server ip_address
```

### Syntax Definitions

- **ip_address**
  The IP address of the NTP server to be added or deleted to the client’s server list. The IP address can be IPv4 or IPv6 address.

- **server_name**
  Fully qualified NTP server domain name.

- **key_id**
  The key identification number that corresponds to the specified NTP server. The value ranges from 0 to 65534. 0 can be used to unconfigure the key ID.

- **minpoll poll**
  It specifies the minimum polling interval for NTP messages, in seconds. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$). The minimum poll interval defaults to 6 (64 s), but can be decreased by the minpoll option to a lower limit of 3 (8 s) and an upper limit of 17 (36.4h).

- **maxpoll poll**
  It specifies the maximum polling interval for NTP messages, in seconds. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the maximum poll time would be 16 seconds ($2^4 = 16$). The maximum poll interval defaults to 10 (1,024 s), but can be increased by the maxpoll option to an upper limit of 17 (36.4h) and a lower limit of 3 (8 s). The maxpoll must not be less than the minpoll value.

- **version**
  The version of NTP being used. This will be 1, 2, 3, or 4.

- **prefer**
  Marks this server as the preferred server. A preferred server’s timestamp will be used before another server.

- **burst**
  Enables burst mode. The burst mode allows the exchange of eight NTP messages (instead of one) when the server is reachable and at each poll interval to achieve faster synchronization. The spacing between the first and the second packet is 16 seconds to allow a modem call to complete, while the spacing between the remaining packets is 2 seconds.

- **iburst**
  Enables initial burst (iburst) mode. The iburst mode allows immediate exchange of eight NTP messages (instead of one) when the server is unreachable and at each poll interval, to achieve faster initial synchronization acquisition. The spacing between the packets is 16 seconds to allow a modem call to complete. Once the server is reachable, the spacing between the packets is 2 seconds.

- **preempt**
  Enables the preemption mode for the server rather than the default persistent.
Network Time Protocol Commands

Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>4</td>
</tr>
<tr>
<td>minpoll</td>
<td>poll 6</td>
</tr>
<tr>
<td>maxpoll</td>
<td>poll 10</td>
</tr>
<tr>
<td>prefer</td>
<td>not preferred</td>
</tr>
<tr>
<td>burst</td>
<td>no burst</td>
</tr>
<tr>
<td>iburst</td>
<td>no iburst</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9900</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use the no form of this command to clear an NTP server from the list of configured servers.
- To configure NTP in the client mode you must first define the NTP servers. Up to 12 NTP servers may be defined.
- Either an IP address or domain name for the specified server can be entered.
- The NTP key identification is an integer. It corresponds to an MD5 authentication key contained in an authentication file (.txt) located on the server. This file must be on both the server and the local switch, and match, for authentication to work. Enter the key identification using the key keyword if the server is set to MD5 authentication.
- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.
- Use the version keyword to set the correct version of NTP.
- Use the minpoll keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered. Therefore, if 4 were entered, the minimum poll time would be 16 seconds ($2^4 = 16$). The client will poll the server for a time update when the minpoll time is exceeded.
- Use the maxpoll keyword to specify the maximum polling interval for NTP messages. This number is determined by raising 2 to the power of the number entered. The maximum poll interval defaults to 10 (1,024 s), but can be increased by the maxpoll option to an upper limit of 17 (36.4 h) and a lower limit of 3 (8 s). The maxpoll must not be less than the minpoll value.
• NTP authentication must be disabled before adding or removing an NTP server.

• Burst mode of operation improves timekeeping quality with the server command and iburst mode of operation is designed to speed the initial synchronization acquisition with the server command.

• When preempt is enabled, the specified server is marked unavailable for selection if any error (authentication failure) is detected on a connection between the local device and reference clock. The server is marked available for selection if no other connections are available and no error is detected on the connection between the local device and reference clock.

Examples

-> ntp server 1.1.1.1
-> ntp server 4100:1000::124
-> ntp server 0.pool.ntp.org
-> ntp server 1.1.1.1 key 1
-> ntp server 1.1.1.1 version 4
-> ntp server 0.pool.ntp.org minpoll 5
-> ntp server 0.pool.ntp.org maxpoll 6
-> ntp server 1.1.1.1 burst
-> ntp server 1.1.1.1 iburst
-> ntp server 1.1.1.1 preempt
-> no ntp server 1.1.1.1

Release History

Release 7.1.1; command was introduced.
Release 8.5R4: server name, maxpoll, burst, iburst, preempt keywords added.
Release 8.7R3; NTP support for IPv6 added.

Related Commands

ntp client
  Enables or disables NTP operation on the switch.

show ntp client server-list
  Displays a list of the servers with which the NTP client synchronizes.

show ntp server status
  Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

alaNtpPeerTable
  alaNtpPeerAddressType
  alaNtpPeerAddress
  alaNtpPeerIpAddress
  alaNtpPeerType
  alaNtpPeerAuth
  alaNtpPeerVersion
  alaNtpPeerMinpoll
  alaNtpPeerPrefer
  alaNtpPeerAdmin
  alaNtpPeerName
  alaNtpPeerStratum
  alaNtpPeerBurst
  alaNtpPeerIBurst
  alaNtpPeerPreempt
  alaNtpPeerMaxpoll
alaNtpPeerInetAddressType
alaNtpPeerInetAddress
**ntp server synchronized**

Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.

**Syntax Definitions**

N/A

**Defaults**

By default, NTP synchronization is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The NTP protocol discards the NTP servers that are unsynchronized. However, the unsynchronized NTP servers are used as network time sources.

**Examples**

```
-> ntp server synchronized
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated.

**Related Commands**

- **ntp server unsynchronized** Disables an NTP client from invoking tests for NTP server synchronization. This allows the NTP client to synchronize with unsynchronized NTP servers in the network.

**MIB Objects**

alaNtpConfig
alaNtpPeerTests
ntp server unsynchronized

Disables an NTP client from invoking tests for NTP server synchronization. This allows the NTP client to synchronize with unsynchronized NTP servers in the network.

ntp server unsynchronized

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

When NTP peer synchronization tests are disabled, the NTP client is able to synchronize with either an NTP peer that is not synchronized with an atomic clock or a network of NTP servers that will finally synchronize with an atomic clock.

Examples

- ntp server unsynchronized

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated.

Related Commands

ntp server synchronized Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.

MIB Objects

alaNtpConfig
alaNtpPeerTests
**ntp client**

Enables or disables NTP time synchronization discipline.

```plaintext
ntp client admin-state {enable | disable}
```

### Syntax Definitions

- **enable**: Enables NTP.
- **disable**: Disables NTP.

### Defaults

NTP protocol is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use this command to enable or disable NTP. Before NTP can be enabled, an NTP server must be specified using the `ntp server` command. Up to 12 NTP servers may be defined.

- It is not necessary to specify an NTP server if the NTP client will only receive time updates from NTP broadcast servers.

- NTP client will not synchronize with an unsynchronized NTP server (Stratum 16).

### Examples

```
-> ntp client enable
-> ntp client disable
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

**ntp server**

Specifies an NTP server from which the switch will receive updates.

**MIB Objects**

alaNtpEnable
**ntp src-ip preferred**

Configures a source IP address to use as the source for NTP packets.

```
ntp src-ip preferred {default | no-loopback0 | ip_address}
no ntp src-ip preferred
```

**Syntax Definitions**

- **default**
  
  The Loopback0 address, if configured, will be used for the source IP address field. If no Loopback0 is configured, the EMP-VC IP address will be used. If no EMP-VC IP address is configured, the preferred IP address will be used. If no preferred IP address is configured the first available IP address on the switch will be used.

- **no-loopback0**
  
  The Loopback0 address will not be used for the source IP address field and either the preferred IP address (if configured) or the first available IP address on the switch will be used.

- **ip_address**
  
  The IP address to be used in the source IP field.

**Defaults**

By default, the NTP source IP preferred setting is set to the `default` parameter.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- By default The Loopback0 address, if configured, will be used for the source IP address.
- If no Loopback0 is configured, the VC-EMP IP address will be used for the source IP address.
- If no VC-EMP IP address is configured, the preferred IP address will be used for the source IP address.
- If no preferred IP address is configured the first available IP address on the switch will be used as the source IP address.
- When configuring a preferred IP address, that address must already exist on the switch.
- If the configured preferred IP address is the same as the IP address that would have been automatically chosen by the switch, then the ‘ntp src-ip preferred’ command will not be included in the output of the ‘configuration snapshot’ command since only non-default settings are included in the output.
• Use the **no** form of this command to clear a specific IP address and change the behavior back to default.

**Examples**

-> ntp src-ip preferred 192.168.10.1  
-> ntp src-ip preferred no-loopback0  
-> ntp src-ip preferred default

**Release History**

Release 7.1.1; command was introduced.  
Release 7.3.4; command deprecated.

**Related Commands**

**show ntp status** Display the NTP configuration and status.

**MIB Objects**

N/A
**ntp broadcast-client**

Enables or disables the NTP client to receive time updates from NTP broadcast servers.

```
ntp broadcast-client {enable | disable}
```

### Syntax Definitions

- **enable**
  - Enables the client broadcast mode.

- **disable**
  - Disables the client broadcast mode.

### Defaults

Broadcast mode is disabled by default.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Broadcast mode is intended for operation on networks with numerous workstations and where the highest accuracy is not required. In a typical scenario, one or more time servers on the network broadcast NTP messages that are received by NTP hosts. Correct time is determined from this NTP message based on a pre-configured latency or broadcast delay in the order of a few milliseconds.

- In order to configure NTP in broadcast client mode, it is required to define the network server to client broadcast delay.

### Examples

```
-> ntp broadcast-client enable
-> ntp broadcast-client disable
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

**ntp broadcast-delay** Sets the broadcast delay time in microseconds.

**MIB Objects**

alaNtpBroadcastEnable
**ntp broadcast-delay**

Sets the broadcast delay time in microseconds of received NTP broadcast messages.

**Syntax Definitions**

*milliseconds* The number of microseconds for the broadcast delay.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliseconds</td>
<td>4000</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When running in the NTP client broadcast mode, a broadcast delay must be set. The broadcast delay is the number of microseconds added to the timestamp received from a broadcast NTP server.

**Examples**

- `ntp broadcast-delay 1000`
- `ntp broadcast-delay 10000`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ntp broadcast** Enables or disables the client’s broadcast mode.

**MIB Objects**

- `alaNtpBroadcastDelay`
ntp key

Labels the specified authentication key identification as trusted or untrusted.

ntp key key [trusted | untrusted]

Syntax Definitions

key
The key number matching an NTP server.

trusted
Signifies that the specified key is trusted and can be used for authentication.

untrusted
Signifies that the specified key is not trusted and cannot be used for authentication. Synchronization will not occur with an untrusted authentication key.

Defaults

By default, all authentication key are untrusted.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Authentication keys are stored in a key file and loaded into memory when the switch boots. The keys loaded into memory are not trusted until this command is used. The location of the file containing set of generated authentication keys is /flash/network/ntp.keys.

- Once the keys are loaded into software (on boot up of the switch), they must be activated by being labeled as trusted. A trusted key will authenticate with a server that requires authentication as long as the key matches the server key.

- New keys must be added manually to the key file. A newly added key will not be loaded into the switch software until the `ntp key load` command is issued, or the switch is rebooted.

- An authentication key is composed of a 32-bit integer and 32-byte string of characters. The integer format is hexadecimal. For an NTP message to be authenticated the NTP client authentication key must match the key configured at the NTP server. This means the authentication keys must be distributed in advance of configuring the NTP client. If authentication is disabled but authentication key is present, the association will still be unauthenticated.

- By default all keys read from the ntp.conf key file are untrusted therefore keys must be set to ‘trusted’ status to allow NTP to use the key for authentication.
Examples

-> ntp key 5 trusted
-> ntp key 2 untrusted

Release History

Release 7.1.1; command was introduced.

Related Commands

- **ntp key**: Sets the public key the switch uses when authenticating with the specified NTP server.
- **ntp client**: Enables or disables NTP operation on the switch.

MIB Objects

- **alaNtpAccessKeyIdTable**
  - **alaNtpAccessKeyIdKeyId**
  - **alaNtpAccessKeyIdKeyId**
  - **alaNtpAccessKeyIdTrust**
**ntp key load**

Loads the current key file into memory.

**ntp key load**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command reloads the key file into the switch memory. This allows for new keys in the key file to be added to the list of keys the switch can use for authentication.
- Newly added keys must be labeled as trusted with the `ntp key` command before being used for authentication.
- By default, all authentication keys are untrusted therefore reloading a key file will change any current trusted keys to untrusted status.
- The file ntp.keys is used during the establishment of a set of authentication keys that are used by the NTP protocol. The location of this file is fixed in directory /flash/network.

**Examples**

-> ntp key load

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**ntp key**  
Labels the specified authentication key identification as trusted or untrusted.

**ntp server**  
Specifies an NTP server from which this switch will receive updates.

MIB Objects

`alaNtpAccessRereadkeyFile`
**ntp authenticate**

Enables or disables the authentication on a configured NTP server.

```
ntp authenticate {enable | disable}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables authentication for NTP server.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables authentication for NTP server.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, NTP authentication is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to enable or disable authentication for NTP server.
- Before NTP authentication is enabled, NTP operation should be enabled by using `ntp client` command.
- Before enabling the NTP operation, NTP server must be specified using the `ntp server` command.
- NTP authentication must be disabled before adding or removing an NTP server.

**Examples**

```
-> ntp authenticate enable
-> ntp authenticate disable
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **show ntp status**
  Displays the information about the current NTP status.

MIB Objects

- **alaNtpAuthenticate**
**ntp master**

Specifies the stratum value for unsynchronized switch to act as an authoritative NTP source.

**ntp master stratum_number**

---

### Syntax Definitions

**stratum_number**

Integer value ranging from 2 to 16.

---

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>stratum_number</td>
<td>16</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

- Use this command to synchronize improved clocks with lower strata value if any of the trustworthy NTP sources comes up.
- Use default value of 16 if switch is not synchronized with itself.
- When the switch is synchronized, the stratum number should correspond to peer/server.

---

### Examples

```
-> ntp master 4
```

---

### Release History

Release 7.1.1; command was introduced.
Release 8.5R4; command deprecated.
**Related Commands**

`show ntp status`  
Displays current NTP status.

**MIB Objects**

`alaNtpConfig`

`alaNtpSysStratum`
ntp interface

Enables or Disables NTP server functionality for an interface.

**ntp interface** {interface_ip} {enable | disable}

### Syntax Definitions

- **interface_ip**
  - IP address of an interface on which NTP server functionality is to be disabled. The IP address can be an IPv4 or IPv6 address.
- **enable**
  - Enables NTP server functionality on an interface.
- **disable**
  - Disables NTP server functionality on an interface.

### Defaults

By default, NTP server functionality is enabled on all the interfaces.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use this command to enable or disable the incoming NTP request.
- Disabling the NTP server functionality drops the NTP request on an interface and synchronization information is not sent out.

### Examples

- `-> ntp interface 10.10.10.1 disable`
- `-> ntp interface 10.10.10.1 enable`
- `-> ntp interface 4100:1000::125 enable`
- `-> ntp interface 4100:1000::125 disable`

### Release History

Release 7.1.1; command was introduced.
Release 8.7R3; NTP support for IPv6 added.
Related Commands

show ntp status  Displays current NTP status.

MIB Objects

alaNtpInterfaceDisabledTable
  alaNtpInterfaceDisabledIpAddressType
  alaNtpInterfaceDisabledIpAddress
  alaNtpInterfaceDisabledRestrictions
  alaNtpInterfaceDisabledRowStatus
**ntp max-associations**

Configures the maximum number of associations on the switch.

`ntp max-associations number`

**Syntax Definitions**

`number`  
Maximum no of client/server and peer associations. Integer value ranging from 0 to 512.

**Defaults**

By default, 128 associations are allowed on the switch.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Released</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to restrict the number of client/server and peer association.
- The command can be used to change the default value of 128 to any value between 0 to 512.
- The command protects the switch from overwhelming with the NTP requests. When the limit is reached, trap is sent to indicate the switch.

**Examples**

```
-> ntp max-associations 20
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.6R2; max value increased to 512.
**Related Commands**

*show ntp status*  
Displays current NTP status.

**MIB Objects**

alaNtpConfig

alaNtpMaxAssociation
**ntp broadcast**

Enables NTP to broadcast synchronized information to all the clients in the subnet in the configured interval.

```
ntp broadcast {broadcast_addr} [version version] [minpoll poll_interval]
no ntp broadcast {broadcast_addr}
```

### Syntax Definitions

- `broadcast_addr`: Subnet for which broadcast updates are regularly sent.
- `version`: NTP version on which the broadcast updates are sent out on the subnet for the clients. Value is 3 or 4.
- `poll_interval`: Polling interval for NTP broadcast message. This value is measured in seconds.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>version</code></td>
<td>4</td>
</tr>
<tr>
<td><code>poll_interval</code></td>
<td>6</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

- Use this command to configure NTP to act in broadcast server mode.
- Use the `no` form of this command to remove the configured broadcast servers. This also disables NTP synchronization information being sent for that broadcast subset.
- The NTP broadcast address needs to defined to enable NTP broadcast mode. A maximum of 3 broadcast addresses can be configured.
- Use the `version` keyword to set the correct version of NTP.
- Use the `minpoll` keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered.
**Examples**

```
-> ntp broadcast 10.145.59.255 version 4 minpoll 5
-> no ntp broadcast 10.145.59.255
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **ntp broadcast** Enables or disables the client’s broadcast mode.
- **ntp broadcast-delay** Sets the broadcast delay time in microseconds

**MIB Objects**

- `alaNtpPeerTable`
  - `alaNtpPeerType`
  - `alaNtpPeerVersion`
  - `alaNtpPeerMinpoll`
**ntp peer**

Configures NTP to operate in the symmetric active peering mode. This also enables the establishment of an active symmetric association with the specified remote peer.

```
ntp peer {ip_address} [key key_id] [version version] [minpoll poll_interval]
no ntp peer {ip_address}
```

**Syntax Definitions**

- `ip_address` IP address of the remote peer. The IP address can be IPv4 or IPv6 address.
- `key_id` Authentication key for the remote peer.
- `version` NTP packet version to be used for the peer association.
- `poll_interval` Polling interval for NTP broadcast message. Poll interval which when expires, packets will be sent to the peer.

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>4</td>
</tr>
<tr>
<td>poll_interval</td>
<td>6</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use `no` form of this command to remove the peers that are configured to act in symmetric active mode. This command deletes the symmetric active association with the remote peer.
- Use the `version` keyword to set the correct version of NTP.
- Use the `minpoll` keyword to set the minimum poll time for the server. This number is determined by raising 2 to the power of the number entered.
- The command should not be used for `b(Broadcast), m(Multicast) or r(Reference clock address 127.127.x.x)`.
- `ip-address` is the mandatory parameter to be entered in the command while `key id` is the optional parameter. If `key id` is not specified, then peering will not be authenticated.
Examples

-> ntp peer 172.18.16.112
-> ntp peer 4100:1000::124
-> no ntp peer 172.18.16.112

Release History

Release 7.1.1; command was introduced.
Release 8.7R3; NTP support for IPv6 added.

Related Commands

show ntp peers
Displays current NTP peer association.

MIB Objects

alaNtpPeerTable
  alaNtpPeerAddressType
  alaNtpPeerAddress
  alaNtpPeerIpAddress
  alaNtpPeerType
  alaNtpPeerAuth
  alaNtpPeerVersion
  alaNtpPeerMinpoll
  alaNtpPeerPrefer
  alaNtpPeerAdmin
  alaNtpPeerName
  alaNtpPeerStratum
  alaNtpPeerBurst
  alaNtpPeerIBurst
  alaNtpPeerPreempt
  alaNtpPeerMaxpoll
  alaNtpPeerInetAddressType
  alaNtpPeerInetAddress
ntp vrf-name

Sets the VRF to be used for all NTP operations (both client and server).

**ntp vrf-name name**

### Syntax Definitions

*name* The name of the VRF to be used for all NTP operations.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>default</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

-> ntp vrf-name vrf1

### Release History

Release 7.3.1; command introduced.

### Related Commands

- **show ntp status** Displays the information about the current NTP status.
- **show ntp client** Displays information about the current client NTP configuration.

### MIB Objects

alaIpNtpVrfName
show ntp status

Displays the information about the current NTP status.

show ntp status

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This command displays the information about the status of NTP, which is configured along with other global configuration. See the Examples section for more information.

- If the source IP Configuration is done in default or no-loopback0 then the source ip-address will not be displayed in the output of the show ntp status command.

Example

-> show ntp status
Current time:                   Mon, Jan 21 2019  7:31:04.685 (UTC),
Last NTP update:                Mon, Jan 21 2019  7:30:10.160 (UTC),
Server reference:               10.10.10.10,
Client mode:                    enabled,
Broadcast client mode:          disabled,
Broadcast delay (microseconds): 4000,
Stratum:                        4,
Maximum Associations Allowed:   32,
Authentication:                 enabled,
VRF Name:                       default

Current time
The current time for the NTP client.

Last NTP update
The time of the last synchronization with an NTP server.

Server reference
The source of the time signal, which is the address of the NTP server that provided the currently-used time update.

Client mode
Whether the NTP client software is enabled or disabled.
**Network Time Protocol Commands**

- **Broadcast client mode** - What NTP mode the client is running in, either client or broadcast.
- **Broadcast delay** - The number of microseconds in the advertised broadcast delay time. This field is absent if the client broadcast mode is disabled.
- **Stratum** - The stratum of the server. The stratum number is the number of hops from a UTC time source.
- **Max-Association** - Maximum association on the switch that restricts the number of client/server and peer association.
- **Authentication** - Whether Authentication is enabled or disabled.
- **VRF Name** - Name of the VRF.

**Release History**

Release 7.1.1; command introduced.
Release 7.3.1; vrf parameter added.

**Related Command**

- **ntp client** - Enables or disables NTP operation on the switch.
- **ntp server** - Specifies an NTP server from which the switch will receive updates.
- **ntp server synchronized** - Enables an NTP client to invoke tests for NTP server synchronization as specified by the NTP protocol.
- **ntp max-associations** - Configures the maximum number of associations on the switch.
- **ntp master** - Specifies the stratum value for unsynchronized switch.
- **ntp broadcast** - Enables or disables the client’s broadcast mode.
- **show ntp client** - Displays information about the current client NTP configuration.
- **show ntp client server-list** - Displays a list of the servers with which the NTP client synchronizes.
- **show ntp server client-list** - Displays the basic server information for a specific NTP server or a list of NTP servers.

**MIB Objects**

- `alaNtpPeerListTable`
  - `alaNtpPeerShowOriginTime`
  - `alaNtpPeerShowTransmitTime`
  - `alaNtpEnable`
  - `alaNtpBroadcastEnable`
  - `alaNtpBroadcastDelay`
  - `alaNtpPeerTests`
  - `alaNtpPeerStratum`
  - `alaNtpAuthenticate`
  - `alaNtpSrcIpConfig`
  - `alaNtpSrcTp`
  - `alaIpNtpVrfName`
show ntp client

Displays information about the current client NTP configuration.

show ntp client

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays the current configuration parameters for the NTP client. The display is slightly different depending on what has been configured on the client. See the Examples section for more information.

Examples

-> show ntp client

Current time: Mon, Jan 21 2019 7:31:12.505 (UTC),
Last NTP update: Mon, Jan 21 2019 7:30:10.160 (UTC),
Server reference: 10.10.10.10,
Client mode: enabled,
Broadcast client mode: disabled,
Broadcast delay (microseconds): 4000,
VRF Name: default

output definitions

Current time The current time for the NTP client.
Last NTP update The time of the last synchronization with an NTP server.
Server reference The source of the time signal, which is the address of the NTP server that provided the currently-used time update.
Client mode Whether the NTP client software is enabled or disabled.
Broadcast client mode What NTP mode the client is running in, either client or broadcast.
### Output Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast delay</td>
<td>The number of microseconds in the advertised broadcast delay time. This field is absent if the client broadcast mode is disabled.</td>
</tr>
<tr>
<td>VRF Name</td>
<td>Name of the VRF.</td>
</tr>
</tbody>
</table>

### Release History

Release 7.1.1; command was introduced.

### Related Command

**ntp client**

Enables or disables NTP operation on the switch.

### MIB Objects

- `alaNtpLocalInfo`
- `alaIpNtpVrfName`
show ntp client server-list

Displays a list of the servers with which the NTP client synchronizes.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Mode</th>
<th>IP Address</th>
<th>Ver</th>
<th>Key</th>
<th>St</th>
<th>when</th>
<th>poll</th>
<th>reach</th>
<th>Delay</th>
<th>Offset</th>
<th>Disp</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>198.206.181.170</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>895</td>
<td>1024</td>
<td>377</td>
<td>0.167</td>
<td>0.323</td>
<td>0.016</td>
</tr>
<tr>
<td>-</td>
<td>198.206.181.123</td>
<td>4</td>
<td>0</td>
<td>16</td>
<td>591</td>
<td>1024</td>
<td>377</td>
<td>0.000</td>
<td>0.000</td>
<td>0.000</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display tabular information on the current NTP client to server association status.

**Examples**

```
-> show ntp client server-list
Legends: + active peer, - passive peer, = client, * current system peer, ^ broadcast server, ' broadcast client
```

```
Mode | IP Address       | Ver | Key | St | when | poll | reach | Delay | Offset | Disp
---|------------------|-----|-----|----|------|------|-------|-------|--------|------
*    | 198.206.181.170  | 4   | 0   | 2  | 895  | 1024 | 377   | 0.167 | 0.323  | 0.016 |
-    | 198.206.181.123  | 4   | 0   | 16 | 591  | 1024 | 377   | 0.000 | 0.000  | 0.000 |
```

**output definitions**

- **Mode**
  - "+" indicates an active peer
  - "." indicates a passive peer
  - "+" indicates a client
  - "+" indicates current system peer
  - "^" indicates a broadcast server
  - "^" indicates a broadcast client

- **IP Address**
  - The server IP address.

- **Ver**
  - The version of NTP the server is using. Versions 3 and 4 are valid.

- **Key**
  - The NTP server’s public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
output definitions

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>St</td>
<td>The stratum of the server.</td>
</tr>
<tr>
<td>When</td>
<td>Number of seconds passed since last response from remote host.</td>
</tr>
<tr>
<td>Poll</td>
<td>Polling interval to the remote host in seconds.</td>
</tr>
<tr>
<td>Reach</td>
<td>This is a shift register used to determine the reachability status of this peer. This register is displayed to the user in octal values instead of binary, decimal or even hex. The maximum value of an eight-bit binary number is 11111111, which is 377 in octal.</td>
</tr>
<tr>
<td>Delay</td>
<td>The delay received from the server in its timestamp.</td>
</tr>
<tr>
<td>Offset</td>
<td>The offset received from the server in its timestamp.</td>
</tr>
<tr>
<td>Disp</td>
<td>The dispersion value received from the server in its timestamp.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; “When”, “Poll”, “Reach” fields added.

Related Command

**ntp client**

Enables or disables NTP operation on the switch.

MIB Objects

**alaNtpPeerListTable**
show ntp server client-list

Displays the information about the current NTP clients connected to the server.

**show ntp server client-list**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display the tabular information on the current NTP client connected to the server (switch).

**Examples**

```bash
-> show ntp server client-list
IP Address          Ver  Key
---------------------+-----+-----
172.23.0.201         4    0
10.255.24.121        4    0
```

**output definitions**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The client IP address.</td>
</tr>
<tr>
<td>Ver</td>
<td>The version of NTP the server is using. Versions 3 and 4 are valid.</td>
</tr>
<tr>
<td>Key</td>
<td>The NTP server’s public key. This must be accurate and the same as the NTP server or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Related Command

- **show ntp status**  Displays information about the current client NTP configuration
- **ntp client**  Enables or disables NTP operation on the switch.

MIB Objects

- **alaNtpClientListTable**
  - **alaNtpPeerListAddress**
  - **alaNtpPeerVersion**
  - **alaNtpPeerAuth**
**show ntp server status**

Displays the basic server information for a specific NTP server or a list of NTP servers.

```
show ntp server status [ip_address]
```

**Syntax Definitions**

`ip_address` The IP address of the NTP server to be displayed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command displays information on the status of any or all configured NTP servers/peers.
- To display a specific server, enter the command with the server’s IP address. To display all servers, enter the command with no server IP address.

**Examples**

```
-> show ntp server status
IP address = clock3.ovcirrus.com [123.108.200.124],
Host mode = client,
Peer mode = server,
Prefer = no,
Version = 4,
Key = 0,
Stratum = 2,
Minpoll = 6 (64 seconds),
Maxpoll = 10 (1024 seconds),
Poll = 1024 seconds,
when = 283 seconds,
Delay = 0.016 seconds,
Offset = -180.232 seconds,
Dispersion = 7.945 seconds
Root distance = 0.026,
Precision = -14,
Reference IP = 209.81.9.7,
Status = configured : reachable : rejected,
Uptime count = 1742 seconds,
```
Reachability = 1,
Unreachable count = 0,
Stats reset count = 1680 seconds,
Packets sent = 1,
Packets received = 1,
Duplicate packets = 0,
Bogus origin = 0,
Bad authentication = 0,
Bad dispersion = 0,

-> show ntp server status 198.206.181.139
IP address = 198.206.181.139,
Host mode = client,
Peer mode = server,
Prefer = no,
Version = 4,
Key = 0,
Stratum = 2,
Minpoll = 6 (64 seconds),
Maxpoll = 10 (1024 seconds),
Poll = 1024 seconds,
when = 283 seconds,
Delay = 0.016 seconds,
Offset = -180.232 seconds,
Dispersion = 7.945 seconds
Root distance = 0.026,
Precision = -14,
Reference IP = 209.81.9.7,
Status = configured : reachable : rejected,
Uptime count = 1742 seconds,
Reachability = 1,
Unreachable count = 0,
Stats reset count = 1680 seconds,
Packets sent = 1,
Packets received = 1,
Duplicate packets = 0,
Bogus origin = 0,
Bad authentication = 0,
Bad dispersion = 0,
Last Event = peer changed to reachable,

**output definitions**

<table>
<thead>
<tr>
<th>IP address</th>
<th>The server IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host mode</td>
<td>The host mode of this remote association.</td>
</tr>
<tr>
<td>Peer mode</td>
<td>The peer mode of this remote association.</td>
</tr>
<tr>
<td>Prefer</td>
<td>Whether this server is a preferred server or not. A preferred server is used to synchronize the client before a non-preferred server.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of NTP the server is using. Versions 3 and 4 are valid.</td>
</tr>
<tr>
<td>Key</td>
<td>The NTP server’s public key. This must be accurate and the same as the NTP server, or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.</td>
</tr>
<tr>
<td>Stratum</td>
<td>The stratum of the server. The stratum number is the number of hops from a UTC time source.</td>
</tr>
</tbody>
</table>
output definitions (continued)

<table>
<thead>
<tr>
<th>Minpoll</th>
<th>The minimum poll time. The client will poll the server for a time update every time this limit has been exceeded.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maxpoll</td>
<td>The maximum poll time.</td>
</tr>
<tr>
<td>When</td>
<td>Number of seconds passed since last response from remote host.</td>
</tr>
<tr>
<td>Poll</td>
<td>Polling interval to the remote host in seconds.</td>
</tr>
<tr>
<td>Delay</td>
<td>The delay received from the server in its timestamp.</td>
</tr>
<tr>
<td>Offset</td>
<td>The offset received from the server in its timestamp.</td>
</tr>
<tr>
<td>Dispersion</td>
<td>The dispersion value received from the server in its timestamp.</td>
</tr>
<tr>
<td>Root distance</td>
<td>The total round trip delay (in seconds) to the primary reference source.</td>
</tr>
<tr>
<td>Precision</td>
<td>The advertised precision of this association.</td>
</tr>
<tr>
<td>Reference IP</td>
<td>The IP address identifying the peer’s primary reference source.</td>
</tr>
<tr>
<td>Status</td>
<td>The peer selection and association status.</td>
</tr>
<tr>
<td>Uptime count</td>
<td>The time period (in seconds) during which the local NTP server was associated with the switch.</td>
</tr>
<tr>
<td>Reachability</td>
<td>The reachability status of the peer.</td>
</tr>
<tr>
<td>Unreachable count</td>
<td>Number of times the NTP entity was unreachable.</td>
</tr>
<tr>
<td>Stats reset count</td>
<td>The time delay (in seconds) since the last time the local NTP server was restarted.</td>
</tr>
<tr>
<td>Packets sent</td>
<td>Number of packets sent.</td>
</tr>
<tr>
<td>Packets received</td>
<td>Number of packets received.</td>
</tr>
<tr>
<td>Duplicate packets</td>
<td>Number of duplicated packets received.</td>
</tr>
<tr>
<td>Bogus origin</td>
<td>Number of bogus packets.</td>
</tr>
<tr>
<td>Bad authentication</td>
<td>Number of NTP packets rejected for not meeting the authentication standards.</td>
</tr>
<tr>
<td>Bad dispersion</td>
<td>Number of bad dispersions.</td>
</tr>
<tr>
<td>Last Event</td>
<td>The last event.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; when and poll fields added.

Related Command

ntp client  Enables or disables NTP operation on the switch.

MIB Objects

alaNtpPeerListTable
  alaNtpPeerShowStatus
show ntp keys

Displays information about all authentication keys.

show ntp keys

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command displays the information on the current set of trusted authentication keys.

**Examples**

```
-> show ntp keys
Key  Status
======+============
1     untrusted
2     untrusted
3     trusted
4     trusted
5     untrusted
6     untrusted
7     trusted
8     trusted
```

**output definitions**

| Key | Status | The key number corresponding to a key in the key file. Whether the key is trusted or untrusted.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Related Command

ntp key
Labels the specified authentication key identification as trusted or untrusted.

ntp key load
Loads the current key file into memory.

MIB Objects
alaNtpAccessKeyIdTable
show ntp peers

Displays the information about the current status on the NTP peer association.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to display the tabular information on the current NTP peer association status.

Examples

```
-> show ntp peers
IP Address     Ver   Key   St   When   Poll   Reach   Delay    Offset    Disp
-------------+-----+-----+----+------+------+-------+--------+--------+-------
172.23.0.202    4    0     3    895    1024   377     0.300    0.404    0.0024
10.255.24.120   4    0     3    591    1024   377     0.016    0.250    0.0017
```

output definitions

- **IP Address**: Peer IP Address
- **Ver**: The version of NTP the server is using. Versions 3 and 4 are valid.
- **Key**: The NTP server’s public key. This must be accurate and the same as the NTP server or the client switch will not be able to synchronize with the NTP server. A zero (0) means there is no key entered.
- **St**: The stratum of the server.
- **When**: Number of seconds passed since last response from remote host.
- **Poll**: Polling interval to the remote host in seconds.
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reach</td>
<td>This is a shift register used to determine the reachability status of this peer. This register is displayed to the user in octal values instead of binary, decimal or even hex. The maximum value of an eight-bit binary number is 11111111, which is 377 in octal.</td>
</tr>
<tr>
<td>Delay</td>
<td>The delay received from the server in its timestamp.</td>
</tr>
<tr>
<td>Offset</td>
<td>The offset received from the server in its timestamp.</td>
</tr>
<tr>
<td>Disp</td>
<td>The dispersion value received from the server in its timestamp.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.5R4; When, Poll, Reach fields added.

Related Command

- **ntp client** Enables or disables NTP operation on the switch.
- **show ntp status** Displays the information about the current NTP status.
- **show ntp server status** Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

- **alaNtpPeerListTable**
- **alaNtpPeerListAddress**
- **alaNtpPeerVersion**
- **alaNtpPeerAuth**
- **alaNtpPeerStratum**
- **alaNtpPeerListDelay**
- **alaNtpPeerShowOffset**
- **alaNtpPeerListDispersion**
show ntp server disabled-interfaces

Displays the IP addresses of the interfaces on which NTP server is not enabled.

show ntp server disabled-interfaces

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command displays ip interfaces on which currently NTP server functionality is disabled.

Examples

-> show ntp server disabled-interfaces
IP Address
----------
172.23.0.202
10.255.24.120

output definitions

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Peer IP Address</th>
</tr>
</thead>
</table>

Release History

Release 7.1.1; command was introduced.
Related Command

- **show ntp status**
  Displays the information about the current NTP status.

- **show ntp server status**
  Displays the basic server information for a specific NTP server or a list of NTP servers.

MIB Objects

- `alaNtpAccessRestrictedTable`
- `alaNtpPeerListAddress`
Session Management Commands

Session Management commands are used to monitor and configure operator sessions including FTP, Telnet, HTTP (WebView), console, Secure Shell, and Secure Shell FTP on the switch. (See the SNMP Commands chapter for SNMP session commands.) Maximum number of concurrent sessions allowed:

<table>
<thead>
<tr>
<th></th>
<th>OmniSwitch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet(v4)</td>
<td>6</td>
</tr>
<tr>
<td>FTP(v4)</td>
<td>4</td>
</tr>
<tr>
<td>SSH + SFTP(v4)</td>
<td>8</td>
</tr>
<tr>
<td>HTTP</td>
<td>4</td>
</tr>
</tbody>
</table>

MIB information for commands in this chapter are as follows:

Filename: ALCATEL-IND1-SESSION-MGR-MIB.mib
Module: alcatelIND1SessionMgrMIB

Filename: ALCATEL-IND1-SYSTEM-MIB.mib
Module: alcatelIND1SystemMIB

Filename: ALCATEL-IND1-IP-MIB.mib
Module: alcatelIND1IPMIB
A summary of the available commands is listed here:

```
  session login-attempt
  session login-timeout
  session banner
  session timeout
  session session-limit
  session prompt
  session reauthentication
  session xon-xoff
  session cli-auto-complete-space
  show prefix
  user profile save
  user profile reset
  history
  command-log
  kill
  exit
  who
  whoami
  show session config
  show session xon-xoff
  more
  telnet
  ssh
  ssh login-grace-time
  ssh enforce-pubkey-auth
  ssh strong-ciphers
  ssh strong-hmacs
  installsshkey
  revokesshkey
  show command-log status
  show telnet
  show ssh
```
session login-attempt

Sets or resets the number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.

`session login-attempt integer`

**Syntax Definitions**

`integer` The number of times the user can attempt to log in to the switch before the TCP connection is closed. Valid range is 1 to 10.

**Defaults**

Default is 3 login attempts.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> session login-attempt 5`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- `show session config` Displays Session Manager information such as banner file name, session timeout value, and default prompt value.
- `session login-timeout` Sets or resets the amount of time the user can take to accomplish a successful login to the switch.
- `session timeout` Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

**MIB Objects**

- `sessionMgr`  
  - `sessionLoginAttempt`

**session login-timeout**

Sets or resets the amount of time the user can take to accomplish a successful login to the switch. If the timeout period is exceeded, the TCP connection is closed by the switch.

**session login-timeout seconds**

---

**Syntax Definitions**

seconds  
The number of seconds the switch allows for the user to accomplish a successful login. Valid range is from 5 to 600 seconds.

**Defaults**

Login timeout default is 55 seconds.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

`-> session login-timeout 30`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

**show session config**
Displays Session Manager information such as banner file name, session timeout value, default prompt value, login timer, and login attempt number.

**session login-attempt**
Sets or resets the number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.

**session timeout**
Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

**MIB Objects**

**sessionMgr**

**sessionLoginTimeout**
### session banner

Sets or resets the file name of the user–defined banner. The banner is a welcome banner that appears after the user successfully logs onto the switch.

```
session {cli | ftp | http} banner file_name

no session {cli | ftp | http} banner
```

#### Syntax Definitions

- **cli**
  - Creates/modifies the CLI banner file name.
- **ftp**
  - Creates/modifies the FTP banner file name.
- **http**
  - Creates/modifies the HTTP banner file name.
- **file_name**
  - Banner file name including the path from the switch’s /flash directory. The maximum length of the filename and path is 255 characters.

#### Defaults

- A default banner is included in one of the switch’s image files. It is automatically displayed at login so no configuration is needed.
- The user has the option of defining a custom supplementary banner or of using the default banner.

#### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

- The **no session banner** command is used to disable a user defined session banner file from displaying when you log onto the switch.
- The **session banner** command is used to configure or modify the banner file name. You must use a text editor to edit the file containing the banner text.
- The banner file must be manually copied to each unit in a VC.

#### Examples

```
-> session cli banner /switch/banner.txt
```

#### Release History

Release 7.1.1; command was introduced.
**Related Commands**

*show session config*  
Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

**MIB Objects**

SessionConfigTable  
  SessionType  
  SessionBannerFileName
**session timeout**

Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface. When the switch detects no user activity for this period of time, the user is logged off the switch.

```
session {cli | http | ftp} timeout minutes
```

### Syntax Definitions

- `cli`: Sets the inactivity timeout for CLI sessions.
- `http`: Sets the inactivity timeout for HTTP sessions.
- `ftp`: Sets the inactivity timeout for FTP sessions.
- `minutes`: Inactivity timeout value (in minutes). Valid range 1 to 59623.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>4</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
+-----------+---------+---------+---------+---------+---------+---------+---------+---------+---------+---------+---------+
| 6360      | 6465    | 6560    | 6570M   | 6860    | 6860N   | 6865    | 6900    | 6900    | 9900    | 6900    | 9900    |
| Yes       | Yes     | Yes     | Yes     | Yes     | Yes     | Yes     | Yes     | Yes     | Yes     | Yes     | Yes     |
+-----------+---------+---------+---------+---------+---------+---------+---------+---------+---------+---------+---------+
```

### Usage Guidelines

- The inactivity timer value may be different for each type of interface, such as CLI (Console, Telnet), HTTP (including WebView), and FTP.
- If you change the timer, the new value does not affect current sessions; the new timer is applied to new sessions only.

### Examples

```
-> session cli timeout 5
```

### Release History

Release 7.1.1; command was introduced.
Related Commands

**show session config**  Displays Session Manager information, such as banner file name, session timeout value, and default prompt value.

MIB Objects

`SessionConfigTable`
  `SessionType`
  `SessionInactivityTimerValue`
**session session-limit**

Configures the concurrent session limit for FTP, SSH, Telnet and HTTP or HTTPS.

```
session {ftp | ssh | telnet | http} session-limit num
```

### Syntax Definitions

- **ftp**
  - Sets the number of concurrent session for FTP sessions. Valid range 1 to 4.

- **ssh**
  - Sets the number of concurrent session for ssh sessions. Valid range 1 to 8.

- **telnet**
  - Sets the number of concurrent session for telnet sessions. Valid range 1 to 6.

- **http**
  - Sets the number of concurrent session for http or https sessions. Valid range 1 to 32.

- **num**
  - The concurrent session limit.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>4</td>
</tr>
<tr>
<td>ssh</td>
<td>8</td>
</tr>
<tr>
<td>telnet</td>
<td>6</td>
</tr>
<tr>
<td>http</td>
<td>32</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

### Usage Guidelines

The access is denied when the number of sessions exceed the configured session-limit.

### Examples

- `-> session ftp session-limit 2`
- `-> session ssh session-limit 4`
- `-> session telnet session-limit 3`
- `-> session http session-limit 20`
**Release History**

Release 8.9R2; command was introduced.

**Related Commands**

`show session config` Displays Session Manager information, such as banner file name, session timeout value, and default prompt value.

**MIB Objects**

SessionConfigTable

- sessionFtpLimitNum
- sessionSshLimitNum
- sessionTelnetLimitNum
- sessionHttpLimitNum
**session prompt**

Configures the default CLI prompt for console and Telnet sessions. The prompt is the symbol and/or text that appears on the screen in front of the cursor.

```
session prompt default [string]
```

---

**Syntax Definitions**

*string* Prompt string. Maximum length 31 characters.

---

**Defaults**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>string</td>
<td>-&gt;</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The new prompt will not take effect until you log off and back onto the switch.

---

**Examples**

```
-> session prompt default -->
```

---

**Release History**

Release 7.1.1; command was introduced.

---

**Related Commands**

- `show session config` Displays Session Manager information such as banner file name, session timeout value, and default prompt value.

---

**MIB Objects**

- `SessionConfigTable`  
  - `SessionType`  
  - `sessionDefaultPromptString`
session reauthentication

Configures the timeout interval to reauthenticate for TACACS+ session.

    session reauthentication [minutes]

Syntax Definitions

minutes    The number of minutes the switch waits before retrying the TACACS+
            authentication request. The valid range is from 1 to 1200 minutes.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>5</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- By default, the TACACS+ reauthentication timer is enabled. The default interval is 5 minutes.
- The reauthentication is disabled when the interval is configured as 0.
- The reauthentication is enabled when the interval is configured from 1 to 1200.
- The session reauthentication CLI is applicable only for TACACS+ authentication.

Examples

    -> session reauthentication 6
    -> session reauthentication 0

Release History

Release 8.8R1; command was introduced.
Related Commands

**show session config**
Displays Session Manager information such as banner file name, session timeout value, default prompt value and TACACS+ reauthentication interval.

MIB Objects

SessionConfigTable
  SessionType
  sessionReauthenticationInterval
**session xon-xoff**

Enable or disable the XON-XOFF protocol on the console port.

```
session xon-xoff {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables XON-XOFF on the console port.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables XON-XOFF on the console port.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C6/T48C6/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900X48C8/C32E/T24C2/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The switch may interpret noise from an RS232 line as Control-S (XOFF). If the `session console xon-xoff` command is enabled, traffic to the console port may be stopped.

### Examples

```
-> session xon-xoff enable
-> session xon-xoff disable
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- `show session xon-xoff` Displays whether the console port is enabled or disabled for XON-XOFF.

### MIB Objects

- `sessionXonXoffEnable`
**session cli-auto-complete-space**

Enable or disable the CLI auto completion using space key.

```
  session cli-auto-complete-space {enable | disable}
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables CLI auto completion on the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables CLI auto completion on the switch.</td>
</tr>
</tbody>
</table>

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Auto completion of CLI command can be enabled or disabled using this command.
- With CLI auto-complete feature enabled, the space key can be used for auto completion of the CLI command similar to the TAB key.

### Examples

```
  -> session cli-auto-complete-space enable
  -> session cli-auto-complete-space disable
```

### Release History

Release 8.9R2; command introduced.
**Related Commands**

*show session config*  
Displays session manager configuration information (for example, default prompt, banner file name, inactivity timer, login timer, login attempts, and CLI console shell status).

**MIB Objects**

*sessionCliAutoCompleteSpace*
show prefix

Shows the command prefix (if any) currently stored by the CLI. Prefixes are stored for command families that support the prefix recognition feature.

show prefix

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Prefixes are stored for command families that support the prefix recognition feature. These command families include AAA, Interface, Link Aggregation, QoS, Spanning Tree, and VLAN Management. Other command families do not store a prefix.

### Examples

```
-> show prefix
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

**show prefix**

This command defines the format of the CLI prompt. The prompt can be defined to include the command prefix.

### MIB Objects

N/A
**user profile save**

Saves the user account settings for prompts and the more mode screen setting. These settings will be automatically loaded when the user account logs on.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use this command to save prompt definitions and more mode screen settings for use in future login sessions for the current user account.
- Use the `user profile reset` command to set values to their factory defaults.

**Examples**

-> user profile save

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show prefix**
  Defines substitute command text for the switch’s CLI command keywords.

- **user profile reset**
  Resets the alias, prompt and more values to their factory defaults.

**MIB Objects**

N/A
user profile reset

Resets the alias, prompt, and more values to their factory defaults.

user profile reset

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> user profile reset

Release History

Release 7.1.1; command was introduced.

Related Commands

- show prefix
  Defines substitute command text for the switch’s CLI command keywords.
- user profile save
  Saves the user account settings for aliases, prompts and the more screen.

MIB Objects

N/A
**history**

Displays commands that you have recently issued to the switch. The commands are displayed in a numbered list.

`history number`

---

**Syntax Definitions**

*number*  
The number of commands to display.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C6/T48C6/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X48C4E/V48C8/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>C32E/T24C2/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

N/A

---

**Examples**

```
  -> history
  1 show cmm
  2 show fan
  3 show sensor
```

---

**output definitions**

<table>
<thead>
<tr>
<th>Index</th>
<th>The index of the commands for this CLI session and the associated command.</th>
</tr>
</thead>
</table>

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

Recalls commands listed in the history buffer and displays them at the CLI prompt.

MIB Objects

N/A
Recalls commands listed in the history buffer and displays them at the CLI prompt.

\[ \text{!} \{ \text{!} | n \} \]

**Syntax Definitions**

\[ ! \]
Recalls the last command listed in the history buffer and displays that command at the CLI prompt.

\[ n \]
Identifies a single command in the history buffer by number and displays that command at the CLI prompt.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- You can use the **history** command to list all commands in the history buffer, then use the **!n** syntax to issue a single command from the list.

- When you use **!n** or **!!** to recall a command in the history buffer list, you must press the Enter key to execute the command.

**Examples**

```
-> history
1* show ip interface
2 show vlan
3 show arp
4 clear arp
->!2
show vlan
  vlan  type  admin  oper  ip   mtu   name
  ------------------------+---------+---------+
  1   std    Ena    Ena   Dis  1500   VLAN 1
  10  std    Ena    Ena   Ena  1500   VLAN 10
  12  std    Ena    Ena   Ena  1500   VLAN 12
  14  std    Ena    Ena   Ena  1500   VLAN 14
  30  vip    Ena    Ena   Ena  1500   VIP VLAN 30
  40  vip    Ena    Ena   Ena  1500   VIP VLAN 40
```
4094  mcm    Ena  Ena  Dis  9198  MCM IPC

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

`history`  
Sets the number of commands that will be stored in the CLI history buffer.

**MIB Objects**

N/A
**command-log**

Enables or disables command logging on the switch. When command logging is enabled, a `command.log` is automatically created; this file stores a comprehensive CLI command history for all active sessions since the function was *first* enabled.

```
command-log {enable | disable}
```

**Syntax Definitions**

- **enable**: Creates a file called `command.log` in the switch’s `/flash` directory. Any configuration commands entered on the command line will be recorded to this file until command logging is disabled.

- **disable**: Disables logging of current session commands to the `command.log` file.

**Defaults**

```
<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>
```

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The maximum log file size is 66,402 bytes; the file may hold up to 100 commands.

**Examples**

```
-> command-log enable
-> command-log disable
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

show command-log
Displays the contents of the command.log file.

show command-log status
Shows the current status of the command logging function (i.e., enabled or disabled).

MIB Objects

sessionCliCommandLogEnable
**kill**

Kills an active session. The command takes effect immediately.

`kill session_number`

---

**Syntax Definitions**

`session_number` Number of the session you want to kill.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Use the `who` command to obtain the session number variable.
- You cannot kill your own session.
- You cannot kill a connected session where the user has not yet completed the login process. These sessions appear with username “(at login)” when displayed with the `who` command.

---

**Examples**

`-> kill 3`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**who**
Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP)

MIB Objects

SessionMgr
- sessionIndex
- sessionRowStatus
exit

Ends the current CLI session. If the CLI session to the switch was via Telnet, the connection is closed.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> exit

Release History

Release 7.1.1; command was introduced.

Related Commands

kill

Kills an active session. The command takes effect immediately.

MIB Objects

SessionMgr

sessionIndex

sessionRowStatus
whoami

Displays the current user session.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the who command to display all sessions on the switch.

Examples

-> whoami
Session number = 5
   User name    = admin,
   Access type  = telnet,
   Access port  = NI,
   IP address   = 121.251.17.76,
   Read-only domains = None,
   Read-only families = ,
   Read-Write domains = All ,
   Read-Write families = ,

Output definitions

| Session Number | The session number assigned to the user. |
| User name      | User name.                                |
| Access type    | Type of access protocol used to connect to the switch. |
| Access port    | Switch port used for access during this session. |
| Ip Address     | User IP address.                          |
| Read-only domains | The command domains available with the user’s read-only access. |
| Read-only families | The command families available with the user’s read-only access. |
Session Management Commands

whoami

output definitions

<table>
<thead>
<tr>
<th>Read-Write domains</th>
<th>The command domains available with the user’s read-write access.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-Write families</td>
<td>The command families available with the user’s read-write access.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

who Displays all active login sessions (e.g., Console, Telnet, FTP, HTTP).

kill Kills another user’s session.

MIB Objects

SessionActive

sessionIndex
sessionAccessType
sessionPhysicalPort
sessionUserName
sessionUserReadPrivileges
sessionUserWritePrivileges
sessionUserProfileNumber
sessionUserIpAddress
sessionRowStatus
**who**

Displays all active login sessions.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- You can identify your current login session by using the IP address.
- This command applies to the following session types: Console, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, SNMP.

**Examples**

```
-> who
Session number = 0
  User name   = (at login),
  Access type = console,
  Access port = Local,
  IP address  = 0.0.0.0,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = None,
  Read-Write families = ,

Session number = 5
  User name   = admin,
  Access type = telnet,
  Access port = NI,
  IP address  = 128.251.17.176,
  Read-only domains   = None,
  Read-only families  = ,
  Read-Write domains  = All ,
  Read-Write families = ,
```
output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Number</td>
<td>The session number assigned to the user.</td>
</tr>
<tr>
<td>User name</td>
<td>User name.</td>
</tr>
<tr>
<td>Access type</td>
<td>Type of access protocol used to connect to the switch.</td>
</tr>
<tr>
<td>Access port</td>
<td>Switch port used for access during this session.</td>
</tr>
<tr>
<td>Ip Address</td>
<td>User IP address.</td>
</tr>
<tr>
<td>Read-only domains</td>
<td>The command domains available with the user’s read-only access.</td>
</tr>
<tr>
<td>Read-only families</td>
<td>The command families available with the user’s read-only access.</td>
</tr>
<tr>
<td>Read-Write domains</td>
<td>The command domains available with the user’s read-write access.</td>
</tr>
<tr>
<td>Read-Write families</td>
<td>The command families available with the user’s read-write access.</td>
</tr>
</tbody>
</table>

Possible values for command domains and families are listed here:

Release History

Release 7.1.1; command was introduced.

Related Commands

whoami Displays current user session.

kill Kills another user’s session.

MIB Objects

SessionActive

| SessionIndex
| sessionAccessType
| sessionPhysicalPort
| sessionUserName
| sessionUserReadPrivileges
| sessionUserWritePrivileges
| sessionUserProfileNumber
| sessionUserIpAddress
| sessionRowStatus
**show session config**

Displays session manager configuration information (e.g., default prompt, banner file name, inactivity timer, login timer, login attempts and TACACS+ reauthentication interval).

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the configuration commands detailed in this section to modify any of the values displayed.

**Examples**

```plaintext
-> show session config

Cla Default Prompt   = ->
Cla Banner File Name = ,
Cla Inactivity Timer in minutes = 60,
Ftp Banner File Name = ,
Ftp Inactivity Timer in minutes = 60,
Http Inactivity Timer in minutes = 60,
Login Timer in seconds = 60,
Maximum number of Login Attempts = 2,
Session reauthentication interval in minutes = 1,
Cla auto-complete space = Enable
Ftp session limit = 2,
Ssh session limit = 6,
Telnet session limit = 4,
Http session limit = 8
```

**output definitions**

- **Cla Default Prompt**
  Default prompt displayed for CLI sessions.

- **Cla Banner File Name**
  Name of the file that contains the banner information that will appear during a CLI session.
output definitions (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cli Inactivity Timer in minutes</td>
<td>Inactivity timer value (in minutes) for CLI sessions. The user is logged off when this value is exceeded.</td>
</tr>
<tr>
<td>Ftp Banner File Name</td>
<td>Name of the file that contains the banner information that will appear during an FTP session.</td>
</tr>
<tr>
<td>Ftp Inactivity Timer in minutes</td>
<td>Inactivity timer value (in minutes) for FTP sessions. The user is logged off when this value is exceeded.</td>
</tr>
<tr>
<td>Http Inactivity Timer in minutes</td>
<td>Inactivity timer value (in minutes) for HTTP (including WebView) sessions. The user is logged off when this value is exceeded.</td>
</tr>
<tr>
<td>Login Timer in seconds</td>
<td>The amount of time the user can take to accomplish a successful login to the switch. If the timeout period is exceeded, the TCP connection is closed by the switch.</td>
</tr>
<tr>
<td>Maximum number of Login Attempts</td>
<td>The number of times a user can attempt unsuccessfully to log into the switch before the TCP connection is closed.</td>
</tr>
<tr>
<td>Session reauthentication interval in minutes</td>
<td>The number of minutes the switch waits for before retrying the TACACS+ authentication request.</td>
</tr>
<tr>
<td>Cli auto-complete space</td>
<td>Displays if auto completion of CLI command using space key is enabled or disabled.</td>
</tr>
<tr>
<td>Ftp session limit</td>
<td>Displays the concurrent FTP session limit.</td>
</tr>
<tr>
<td>Ssh session limit</td>
<td>Displays the concurrent SSH session limit.</td>
</tr>
<tr>
<td>Telnet session limit</td>
<td>Displays the concurrent Telnet session limit.</td>
</tr>
<tr>
<td>Http session limit</td>
<td>Displays the concurrent HTTP/HTTPs session limit.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.8R1; **Session reauthentication interval in minutes** field added.
Release 8.9R2; **Cli auto-complete space, Ftp session limit, Ssh session limit, Telnet session limit, and Http session limit** field added.
**Related Commands**

- `session session-limit` Configures the default CLI prompt for console and Telnet sessions.
- `session banner` Sets the file name of the user–defined banner.
- `session timeout` Configures the inactivity timer for a CLI, HTTP (including WebView), or FTP interface.
- `session login-attempt` Sets the number of times a user can attempt to log into the switch unsuccessfully before the TCP connection is closed.
- `session login-timeout` Sets the amount of time the user can take to accomplish a successful login to the switch.
- `session reauthentication` Configures the timeout interval to reauthenticate for TACACS+ session.
- `session cli-auto-complete-space` Enable or disable the CLI auto completion using space key.

**MIB Objects**

SessionConfigTable
  - `sessionType`
  - `sessionBannerFileName`
  - `sessionInactivityTimerValue`
  - `sessionDefaultPromptString`
  - `sessionReauthenticationInterval`
  - `sessionFtpLimitNum`
  - `sessionSshLimitNum`
  - `sessionTelnetLimitNum`
  - `sessionHttpLimitNum`
show session xon-xoff

Displays whether the console port is enabled or disabled for XON-XOFF.

show session xon-xoff

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

The switch may interpret noise from an RS232 line as Control-S (XOFF). If the console port is enabled for XON-XOFF (through the session reauthentication command), traffic to the console port may be stopped.

Examples

-> show session xon-xoff
XON-XOFF Enabled

Release History

Release 7.1.1; command was introduced.

Related Commands

session reauthentication Enables/disables the XON-XOFF protocol on the console port.

MIB Objects

sessionXonXoffEnable
more

Enables the more mode for your console screen display.

more filename

Syntax Definitions

filename The file to display.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- This parameter can also be used to pipe output from the CLI.
- This command is case sensitive.

Examples

- more textfile.txt
- write terminal | more

Release History

Release 7.1.1; command was introduced.

Related Commands

MIB Objects

SystemServices
  systemServicesArg1
  systemServicesAction
**telnet**

Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.

```
[vrf name] telnet {port [default | service_port] | admin-state [enable | disable] | ip_address}
```

### Syntax Definitions

- **name**
  - Name of the VRF.
- **default**
  - Sets the port back to the default of 23.
- **service_port**
  - The TCP service port number. Must be 23 or between 20000-20999.
- **enable | disable**
  - Enables or disables telnet access.
- **ip_address**
  - Specifies the IPv4 or IPv6 address for the Telnet session.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The default directory for Telnet is `/flash`.

### Examples

- `-> telnet port 20999`
- `-> telnet admin-state disable`
- `-> telnet 172.17.6.228`
- `-> vrf vrf1 telnet admin-state enable`

### Release History

Release 7.1.1; command introduced.
Related Commands

ssh
  Invokes the Secure Shell on the switch. A Secure Shell is used to make a secured connection to a remote system or device.

show telnet
  Displays the current configuration specifying the ports the telnet daemons are listening on.

MIB Objects

SystemServices
  systemServicesArg1
  systemServicesAction
  alaIpTelnetAdminStatus
**ssh**

Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.

```bash
[vrf name] ssh {port [default | service_port] | admin-state [enable | disable] | ip_address}
```

### Syntax Definitions

- **name**: Name of the VRF.
- **default**: Sets the port back to the default of 22.
- **service_port**: The TCP service port number. Must be 23 or between 20000-20999.
- **enable | disable**: Enables or disables Secure Shell.
- **ip_address**: Specifies the IPv4 or IPv6 address for the Secure Shell.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You must have a valid username and password for the specified host.

### Examples

- `-> ssh port 20000`
- `-> ssh admin-state disable`
- `-> ssh 172.155.11.211`
  `login as:`
- `-> vrf vrf1 ssh admin-state enable`

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

**telnet**
Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.

**ssh enforce-pubkey-auth**
Invokes Secure Shellv6 on the switch. Secure Shellv6 is used to make a secured connection to an SSHv6 server.

**show command-log**
Displays the status of Secure Shell, SCP/SFTP on the switch.

**show ssh**
Displays the current configuration specifying the ports SSH daemons are listening on.

**MIB Objects**

alaIpSshConfig
alaIpSshAdminStatus
alaIpSshPort
ssh login-grace-time

Configures the duration in which the user has to enter a login password and authenticate for an SSH session.

**ssh login-grace-time seconds**

**Syntax Definitions**

seconds The number of seconds for the grace time period. The range is 30–600.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, the login grace time period is set to 120 seconds.

**Examples**

-> ssh login-grace-time 300
-> ssh login-grace-time 600

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

`show ssh` Displays the current SSH configuration for the switch.

**MIB Objects**

alaIpSshConfig
alaIpSshLoginGraceTime
ssh enforce-pubkey-auth

Enables or disables Secure Shell public key and password authentication. When enabled, password authentication is not allowed.

ssh enforce-pubkey-auth {enable | disable}

Syntax Definitions

| enable   | Enforces only SSH public key authentication. |
| disable  | Enforces both SSH public key and password authentication. |

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> ssh enforce-pubkey-auth enable

Release History

Release 7.1.1; command was introduced.

Related Commands

telnet

Invokes a Telnet session. A Telnet session is used to connect to a remote system or device.

MIB Objects

alaIpSshConfig

alaIpSshPubKeyEnforceAdminStatus
**ssh strong-ciphers**

Enables or disables the enforcement of a Secure Shell (SSH) cipher configuration across a switch reboot.

`ssh strong-ciphers {enable | disable}`

---

### Syntax Definitions

**enable**

Enables the enforcement of an SSH cipher configuration.

**disable**

Disables the enforcement of an SSH cipher configuration.

---

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

---

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

### Usage Guidelines

N/A

---

### Examples

- `ssh strong-ciphers enable`
- `ssh strong-ciphers disable`

---

### Release History

Release 8.3.1; command was introduced.

---

### Related Commands

- `show ssh`
  Displays the current SSH configuration for the switch.

---

### MIB Objects

- `alaIpSshConfig`
- `alaIpSshStrongCiphersAdminStatus`
**ssh strong-hmacs**

Enables or disables the enforcement of a Secure Shell (SSH) HMAC configuration across a switch reboot.

`ssh strong-hmacs {enable | disable}`

---

**Syntax Definitions**

| enable   | Enables the enforcement of an HMAC configuration. |
| disable  | Disables the enforcement of an HMAC configuration. |

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- SSH HMAC refers to message authentication codes that use cryptographic hash functions.
- Enable strong-hmacs will enforce the use of “hmac-sha2-256, hmac-sha2-512” in ssh server.
- Disable will select default hmcas in the configuration.

**Examples**

- `-> ssh strong-hmacs enable`
- `-> ssh strong-hmacs disable`

**Release History**

Release 8.3.1; command was introduced.
Release 8.7R2; hmac-sha1 removed.
Related Commands

**show ssh**

Displays the current SSH configuration for the switch.

MIB Objects

alaIpSshConfig

alaIpSshStrongHmacsAdminStatus
installsshkey

Used to install the public key used for SSH onto the switch.

installsshkey user path

Syntax Definitions

user
The user that the key will be associated with.

path
The location of the key file.

Defaults
N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Be sure the associated private key is stored on the client device.
- Verify that the user that will use SSH is a valid user name on the OmniSwitch.
- Refer to the Switch Management Guide for information on generating the public/private keys.

Examples

```bash
$ -> installsshkey new_ssh_user /flash/system/new_ssh_user_rsa.pub
```

Release History

Release 8.3.1; command was introduced.

Related Commands

- **revokesshkey**
  Used to revoke a key from an SSH user.
- **show ssh**
  Displays the current SSH configuration for the switch.

MIB Objects

N/A
revokesshkey

Used to revoke a key from an SSH user.

`revokesshkey user remote-user`

**Syntax Definitions**

- `user`: The local user name.
- `remote-user`: The user on the remote client device.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> revokesshkey new_ssh_user remote_ssh_user@192.168.10.1
```

**Release History**

Release 8.3.1; command was introduced.

**Related Commands**

- `installsshkey`: Used to install the public key used for SSH onto the switch.
- `show ssh`: Displays the current SSH configuration for the switch.

**MIB Objects**

N/A
show command-log

Displays the contents of the `command.log` file. This file contains a record of all CLI commands executed on the switch since the command logging function was enabled. For more information on enabling and disabling command logging, refer to page 61-26.

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The most recent commands are listed first.
- The command history is archived to the `command.log` file. If this file is removed, the command history will no longer be available. In addition, the `command.log` file has a 66,402 byte capacity. This capacity allows up to 100 commands; if the maximum capacity is reached, only the 100 most recent commands display.

**Examples**

```
-> show command-log
Command : ip interface Marketing address 17.11.5.2 vlan 255
  UserName : admin
  Date     : FRI JAN 09 00:20:01
  Ip Addr  : 128.251.19.240
  Result   : SUCCESS
Command : ip interface "Distribution" 11.255.14.102 vlan 500 local-proxy-arp
  UserName : admin
  Date     : FRI JAN 09 00:19:44
  Ip Addr  : 128.251.19.240
  Result   : ERROR: Ip Address must not belong to IP VLAN 44 subnet
Command : command-log enable
  UserName : admin
  Date     : FRI JAN 09 00:18:49
  Ip Addr  : 128.251.19.240
  Result   : SUCCESS
```
**Output Definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command</strong></td>
<td>The exact syntax of the command, as entered by the user.</td>
</tr>
<tr>
<td><strong>UserName</strong></td>
<td>The name of the user session that entered the command. For more information on different user session names, refer to the user command on page 39-60, or the “Managing Switch User Accounts” chapter in the OmniSwitch AOS Release 8 Switch Management Guide.</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>The date and time, down to the second, when the command was entered.</td>
</tr>
<tr>
<td><strong>IpAddr</strong></td>
<td>The IP address of the terminal from which the command was entered.</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>The outcome of the command entry. Options include SUCCESS and ERROR. For erroneous command entries, the same error details presented by the switch at the time the command was entered are also displayed in the log file.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **command-log** Enables or disables command logging on the switch.
- **show command-log status** Shows the current status of the command logging function (i.e., enabled or disabled).

**MIB Objects**

- `sessionCliCommandLogEnable`
**show command-log status**

Shows the current status of the command logging function (for example, enabled or disabled).

```
show command-log status
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

```
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

N/A

**Examples**

```
-> show command-log status
CLI command logging : Enable
```

**output definitions**

<table>
<thead>
<tr>
<th>CLI command logging</th>
<th>The current status of command logging on the switch. Options include Disable and Enable.</th>
</tr>
</thead>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **command-log** Enables or disables command logging on the switch.

**MIB Objects**

- `sessionCliCommandLogStatus`
**show telnet**

Displays the current configuration specifying the ports the telnet daemons are listening on.

```plaintext
[vrf name] show telnet
```

---

**Syntax Definitions**

```plaintext
name
```

Name of the VRF.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If VRF is specified, the current status of the telnet daemon for the specified VRF is displayed.

**Examples**

```plaintext
vrf1::-> show telnet
Telnet Admin-State = Enabled
Telnet Port = 23
```

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `command-log` Enables or disables command logging on the switch.

**MIB Objects**

- `alaIpTelnetAdminStatus`
- `alaIpTelnetPort`
show ssh

Displays the current configuration specifying the ports on which the SSH daemons are listening.

[vrf name] show ssh

Syntax Definitions

name

Name of the VRF.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

If VRF is specified, the current status of the SSH daemon for the specified VRF is displayed.

Examples

vrf1:---> show ssh
Ssh Admin-State = Enabled
Ssh Port = 22
Ssh Enforce-Pubkey-Auth = Disabled
Ssh Strong-Ciphers = Disabled
Ssh Strong-Hmacs = Disabled
Ssh login-grace-time = 600 seconds

Release History

Release 7.1.1; command was introduced.
Release 8.3.1; Ssh Strong-Ciphers and Ssh Strong-Hmacs fields added.
Release 8.3.1.R02; Ssh login-grace-time field added.
Related Commands

**command-log**

Enables or disables command logging on the switch.

MIB Objects

alaIpSshConfig

- alaIpSshAdminStatus
- alaIpSshPort
- alaIpSshPubKeyEnforceAdminStatus
- alaIpSshStrongCiphersAdminStatus
- alaIpSshStrongHmacsAdminStatus
- alaIpSshLoginGraceTime
This chapter includes descriptions for CLI commands used to manage files on the switch. Several of these commands are used to create, move, and delete both files and directories in the OmniSwitch flash directory. Other commands allow you to change command privileges and to monitor the memory usage on the switch.

MIB information for the system commands is listed here:

**Filename:** ALCATEL-IND1-SYSTEM-MIB.mib  
**Module:** alcatelIND1SystemMIB

**Filename:** ALCATEL-IND1-CHASSIS-MIB.mib  
**Module:** alcatelIND1ChassisMIB

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>File System</th>
<th>cd</th>
<th>pwd</th>
<th>mkdir</th>
<th>rmdir</th>
<th>ls</th>
<th>rm</th>
<th>cp</th>
<th>scp</th>
<th>mv</th>
<th>chmod</th>
<th>fsck</th>
<th>freespace</th>
<th>fsck</th>
<th>newfs</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Services</td>
<td>vi</td>
<td>tty</td>
<td>show tty</td>
<td>tftp</td>
<td>sftp</td>
<td>ftp</td>
<td>show ftp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
cd

Changes the current working directory of the switch.

cd [path]

---

**Syntax Definitions**

*path* Specifies the path to the working directory. If no path is specified, the current directory of the switch is changed to the higher directory level.

---

**Defaults**

The default working directory of the switch is `/flash`.

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Separate the multiple directory names that are part of the path with a slash (/).

---

**Examples**

- `-> cd`
- `-> cd /flash/certified`

---

**Release History**

Release 7.1.1; command introduced.
Related Commands

**pwd**
Displays the current working directory of the switch.

**mkdir**
Creates a new directory.

**rmdir**
Deletes an existing directory.

**ls**
Displays the contents of a specified directory or the current working directory.

**rm**
Displays the contents of a specified directory or the current working directory.

MIB Objects

- `systemServices`
  - `systemServicesWorkingDirectory`
**pwd**

Displays the current working directory of the switch.

**pwd**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `pwd` command can also be used on the secondary CMM.

**Examples**

```
-> pwd
/flash
```

**Release History**

Release 7.1.1; command introduced.
Related Commands

- **cd**
  Changes the current working directory of the switch.

- **mkdir**
  Creates a new directory.

- **rmdir**
  Deletes an existing directory.

- **ls**
  Displays the contents of a specified directory or the current working directory.

- **rm**
  Displays the contents of a specified directory or the current working directory.

MIB Objects

- **systemServices**
  - systemServicesWorkingDirectory
**mkdir**

Creates a new directory.

```
mkdir [options] [path] /dirname
```

---

**Syntax Definitions**

- **options**
  - Use the ‘?’ on the command line for a list of options.
- **path**
  - The path or location in which the new directory is to be created. If no path name is specified, the new directory is created in the current directory.
- **dirname**
  - A user-defined name for the new directory.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Separate the directory names that are part of the path with a slash (/). Refer to the examples below.
- The `mkdir` command can also be used on the secondary CMM.

---

**Examples**

```
-> mkdir test_directory
-> mkdir flash/test_directory
-> mkdir
```


Usage: mkdir [OPTIONS] DIRECTORY...

Create DIRECTORY

Options:

- `-m` Mode
- `-p` No error if exists; make parent directories as needed
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Changes the current working directory of the switch.</td>
</tr>
<tr>
<td>pwd</td>
<td>Displays the current working directory of the switch.</td>
</tr>
<tr>
<td>rmdir</td>
<td>Deletes an existing directory.</td>
</tr>
<tr>
<td>ls</td>
<td>Displays the contents of a specified directory or the current working directory.</td>
</tr>
<tr>
<td>rm</td>
<td>Displays the contents of a specified directory or the current working directory.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- systemServices
  - systemServicesArg1
  - systemServicesAction
**rmdir**

Deletes an existing directory.

```
rmdir [options] dirname
```

### Syntax Definitions

| `options` | Use the ‘?’ on the command line for a list of options. |
| `dirname` | The name of the existing directory to be removed. |

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Separate the directory names that are part of the path with a slash (/). Refer to the examples below.
- This command can also be used on the secondary CMM.

### Examples

```
-> rmdir ./working
-> rmdir flash/working
-> rmdir ?
```


Usage: rmdir [OPTIONS] DIRECTORY...

Remove DIRECTORY if it is empty

Options:

```
-p|--parents     Include parents
--ignore-fail-on-non-empty
```

### Release History

Release 7.1.1; command introduced.
**Related Commands**

- **cd**  
  Changes the current working directory of the switch.

- **pwd**  
  Displays the current working directory of the switch.

- **mkdir**  
  Creates a new directory.

- **ls**  
  Displays the contents of a specified directory or the current working directory.

**MIB Objects**

- **systemServices**
  - **systemServicesArg1**
  - **systemServicesAction**
**ls**

Displays the contents of a specified directory or the current working directory.

`ls [options] [path/filename]`

---

**Syntax Definitions**

- **options**
  Use the ‘?’ on the command line for a list of options.

- **filename**
  Specifies the file or directory path.

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

Separate the multiple directory names that are part of the path with a slash (/).

---

**Examples**

- `ls`
- `ls -l /flash/certified`
- `ls ?`


Usage: `ls [-lAacCdeFilnpRrsTtuwxXh] [FILE]...`

List directory contents

Options:

- `-l` List in a single column
- `-A` Don't list . and ..
- `-a` Don't hide entries starting with .
- `-C` List by columns
- `-c` With -l: sort by ctime
- `--color=[{always,never,auto}]` Control coloring
- `-d` List directory entries instead of contents
- `-e` List full date and time
- `-F` Append indicator (one of */=@|) to entries
- `-i` List inode numbers
- `-l` Long listing format
-n  List numeric UIDs and GIDs instead of names
-p  Append indicator (one of /=@|) to entries
-L  List entries pointed to by symlinks
-R  Recurse
-r  Sort in reverse order
-S  Sort by file size
-s  List the size of each file, in blocks
-T N Assume tabstop every N columns
-t  With -l: sort by modification time
-u  With -l: sort by access time
-v  Sort by version
-w N Assume the terminal is N columns wide
-x  List by lines
-X  Sort by extension
-h  List sizes in human readable format (1K 243M 2G)

Release History

Release 7.1.1; command introduced.

Related Commands

cd       Changes the current working directory of the switch.
pwd      Displays the current working directory of the switch.
mkdir    Creates a new directory.
rmdir    Deletes an existing directory.
rm        Displays the contents of a specified directory or the current working directory.

MIB Objects

systemServices
  systemServicesArg1
  systemServicesAction
**rm**

Permanently deletes an existing file.

```
rm [options] [path/filename]
```

### Syntax Definitions

- **options**: Use the ‘?’ on the command line for a list of options.
- **filename**: Specifies the file or directory path.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.
- Use care when deleting files. Depending on your switch and network configurations, specific configuration and image files must be present for your system to work properly.
- This command can also be used on the secondary CMM.

### Examples

- `-> rm test_config_file`
- `-> rm flash/test_config_file`
- `-> rm ?`


Usage: `rm [OPTIONS] FILE...`

Remove (unlink) FILEs

Options:
- `-i` Always prompt before removing
- `-f` Never prompt
- `-R,-r` Recurse
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`cp`  
Copies an existing file or directory.

**MIB Objects**

`systemServices`
- `systemServicesArg1`
- `systemServicesAction`
**cp**

Copies an existing file. This command can also copy a directory if the `-r` keyword is used.

`cp [options] source destination`

**Syntax Definitions**

- `options` Use the ‘?’ on the command line for a list of options.
- `source` The name of the existing file to be copied.
- `destination` The new user-defined file name for the resulting file copy. If you are copying a file to the same directory as the original, the file name for the copy must be different from the original.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- You should verify that the `/flash` directory of your switch has enough available memory to hold the copies of the files and directories created.
- A file can be copied to a new directory location. Copy of a file can also be created in the same directory that contains the original file.
- Separate the multiple directory names that are part of the path with a slash (`/`). Refer to the examples below.
- This command can also be used on the secondary CMM.

**Examples**

- `cp flash/snapshots/asc.1.snap flash/snapshots/snapshot_copy`
- `cp flash/snapshots/asc.1.snap snapshot_copy`
- `cp asc.1.snap flash/snapshots/snapshot_copy`
- `cp asc.1.snap snapshot_copy`
- `cp ?`


Usage: `cp [OPTIONS] SOURCE DEST`
Copy SOURCE to DEST, or multiple SOURCE(s) to DIRECTORY

Options:
- `-a` Same as `-dpR`
- `-R,-r` Recurse
- `-d,-P` Preserve symlinks (default if `-R`)
- `-L` Follow all symlinks
- `-H` Follow symlinks on command line
- `-p` Preserve file attributes if possible
- `-f` Force overwrite
- `-i` Prompt before overwrite
- `-l,-s` Create (sym)links

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`mv` Moves an existing file or directory to a new location.

**MIB Objects**

`systemServices`
- `systemServicesArg1`
- `systemServicesArg2`
- `systemServicesAction`
scp

Copies an existing file in a secure manner.

```
scp [options] user_name@remote_ip_addr:[path]/source [path]/target

scp [options] [path]/source user_name@remote_ip_addr:[path]/target
```

### Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>options</code></td>
<td>Use the ‘?’ on the command line for a list of options.</td>
</tr>
<tr>
<td><code>user_name@remote_ip_addr:</code></td>
<td>The username along with the IPv4 or IPv6 address of the remote switch.</td>
</tr>
<tr>
<td><code>path/</code></td>
<td>Specifies the path containing the file to be copied and the path where the file will be copied.</td>
</tr>
<tr>
<td><code>source</code></td>
<td>The name of the file(s) to be copied.</td>
</tr>
<tr>
<td><code>target</code></td>
<td>The new user-defined file name for the resulting file copy.</td>
</tr>
</tbody>
</table>

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- This command will prompt you to enter the admin password, and the names and the path of the files being copied will be displayed.
- A file may be copied to a new location; you are not required to copy a file to the same directory that contains the original.
- Separate the multiple directory names that are part of the path with a slash (/). Refer to the examples below.

### Examples

```
-> scp admin@172.17.11.13:/flash/working/Kos.img /flash/working/Kos.img
admin's password for keyboard-interactive method:

Fetching /flash/working/Kos.img to /flash/working/Kos.img
Connection to 172.17.11.13 closed.

-> scp /flash/working/Kos.img admin@172.17.11.13:/flash/working/Kos.img
admin's password for keyboard-interactive method:
```
Uploading /flash/working/Kos.img to /flash/working/Kos.img
Connection to 172.17.11.13 closed.

-> scp admin@172.17.11.13:/flash/working/*.*img /flash/working
admin's password for keyboard-interactive method:

Fetching /flash/working/K2os.img to /flash/working/K2os.img
Fetching /flash/working/Kadvrout.img to /flash/working/Kadvrout.img
Fetching /flash/working/Kbase.img to /flash/working/Kbase.img
Fetching /flash/working/Keni.img to /flash/working/Keni.img
Fetching /flash/working/Kos.img to /flash/working/Kos.img
Fetching /flash/working/Krelease.img to /flash/working/Krelease.img
Fetching /flash/working/Ksecu.img to /flash/working/Ksecu.img
Connection to 172.17.11.13 closed.

-> scp ?
       [-l limit] [-o ssh_option] [-P port] [-S program]
       [[user@]host1:]file1 ... [[user@]host2:]file2

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

`mv` Moves an existing file or directory to a new location.

**MIB Objects**

systemServices
  systemServicesArg1
  systemServicesArg2
  systemServicesAction
**mv**

Moves an existing file or directory to a new location.

`mv [options] source destination`

---

**Syntax Definitions**

- **options**
  - Use the ‘?’ on the command line for a list of options.
- **source**
  - The name of the existing file to be copied.
- **destination**
  - The new user-defined file name for the resulting file copy. If you are copying a file to the same directory as the original, the file name for the copy must be different from the original.

---

**Defaults**

N/A

---

**PlatformsSupported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The `mv` command does not make a copy of the file or directory being moved. To copy a file or directory to the current path or to a new location, use the `cp` command.

- Separate the directory names and file names that are part of the path with a slash (/). Refer to the examples below.

- This command can also be used on the secondary CMM.

---

**Examples**

```
-> mv flash/asc.1.snap flash/backup_files/asc.1.snap
-> mv ?

Usage: mv [OPTIONS] SOURCE DEST
or: mv [OPTIONS] SOURCE... DIRECTORY

Rename SOURCE to DEST, or move SOURCE(s) to DIRECTORY

Options:
  -f  Don't prompt before overwriting
  -i  Interactive, prompt before overwrite
```
Release History

Release 7.1.1; command introduced.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rm</td>
<td>Renames an existing file or directory.</td>
</tr>
<tr>
<td>cp</td>
<td>Copies an existing file or directory.</td>
</tr>
</tbody>
</table>

MIB Objects

systemServices
  systemServicesArg1
  systemServicesArg2
  systemServicesAction
chmod

Changes the write privileges for a specified file.

```
chmod {+w | -w} [path]/file
```

**Syntax Definitions**

- **+w**
  - Enables read-write privileges for the file.
- **-w**
  - Disables write privileges for the file—i.e., the file becomes read-only.
- **path/**
  - The path containing the file for which privileges are being changed.
- **file**
  - The name of the file for which read-write privileges are being changed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can also be used on the secondary CMM.

**Examples**

```
-> chmod +w vlan.config
-> chmod -w flash/backup_configs/vlan.config
```

**Release History**

Release 7.1.1; command introduced.

**Related Commands**

- **freespace**
  - Changes the write privileges for a specified file.

**MIB Objects**

```
systemServices
  systemServicesArg1
  systemServicesAction
```
freespace

Displays the amount of free space available in the /flash directory.

\texttt{freespace [/]flash | /uflash]}

\underline{Syntax Definitions}

<table>
<thead>
<tr>
<th>/flash</th>
<th>The amount of free space is shown for the /flash directory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>/uflash</td>
<td>The amount of free space is shown for the /uflash directory.</td>
</tr>
</tbody>
</table>

\underline{Defaults}

N/A

\underline{Usage Guidelines}

N/A

\underline{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

\begin{center}
\begin{tabular}{|c|c|c|c|c|c|c|c|c|c|}
\hline
\hline
Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes & Yes \\
\hline
\end{tabular}
\end{center}

\underline{Examples}

\begin{itemize}
\item \texttt{-> freespace /flash}
\item \texttt{/flash 3143680 bytes free}
\item \texttt{-> freespace}
\item \texttt{/flash 3143680 bytes free}
\end{itemize}

\underline{Release History}

Release 7.1.1; command introduced.
Related Commands

**fsck**
Performs a file system check, including diagnostic information in the event of file corruption. If the `fsck` command detects a problem with the `/flash` file system, a message is displayed indicating the problem, along with any steps needed to resolve it.

MIB Objects

- `SystemFileSystemTable`
  - `systemFileSystemFreespace`
**fsck**

Performs a file system check, including diagnostic information in the event of file corruption.

```bash
fsck /uflash {repair | no-repair}
```

### Syntax Definitions

- **/uflash**
  - Indicates that the file system check will be performed on the `/uflash` directory.
- **repair**
  - Attempt to repair any problems found.
- **no-repair**
  - Do not attempt to repair any problems found.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command provides the option to automatically repair errors.

### Examples

```bash
-> fsck /uflash repair
/uflash/  - disk check in progress ..
/uflash/  - Volume is OK
```

```
  total # of clusters: 14,773
  # of free clusters:  4,132
  # of bad clusters:  0
  total free space: 8,264 Kb
  max contiguous free space: 5,163,008 bytes
  # of files:  46
  # of folders: 3
  total bytes in files: 21,229 Kb
  # of lost chains: 0
  total bytes in lost chains: 0
```
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

**freespace**

Displays the amount of free space available in the `/flash` directory.

**MIB Objects**

systemServices

  systemServicesArg1

  systemServicesAction
newfs

Deletes the complete /uflash file system and all files within it, replacing it with a new, empty /uflash file system. Use this command when you want to reload all files in the file system or in the unlikely event that the /uflash file system becomes corrupt.

newfs /uflash

Syntax Definitions

/uflash This indicates that the complete file system will be replaced.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- It is recommended that you preserve all required image and configuration files by saving them to a remote host before executing the newfs command.

- Do not power-down the switch after running the newfs command until you reload all required image and configuration files.

Examples

-> newfs /uflash

Release History

Release 7.1.1; command introduced.

Related Commands

N/A
**MIB Objects**

systemServices
  systemServicesArg1
  systemServicesAction
**vi**

Launches the switch’s Vi text editor. The Vi file editor allows you to view or edit the contents of a specified text file.

`vi [options] [path]/filename`

---

**Syntax Definitions**

- **options**: Use the ‘?’ on the command line for a list of options.
- **path/**: The path (i.e., location) containing the file being viewed or edited. If no path is specified, the command assumes the current directory.
- **filename**: The name of the existing file being viewed or edited.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Until you exit the switch’s file editor, all keystrokes will be passed to the text editor rather than the switch’s command line.

- This command can also be used on the secondary CMM.

**Examples**

```
-> vi test_config_file
-> vi ?

Usage: vi [OPTIONS] [FILE]...

Edit FILE

Options:
- -c Initial command to run ($EXINIT also available)
- -R Read-only
- -H Short help regarding available features
```
**Release History**

Release 7.1.1; command introduced.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tty</td>
<td>Displays current TTY settings.</td>
</tr>
</tbody>
</table>

**MIB Objects**

- `systemServices`
  - `systemServicesTtyLines`
  - `systemServicesTtyColumns`
tty

Specifies the number of lines and columns to be displayed on the terminal screen while the switch is in the edit file mode.

`tty lines columns`

### Syntax Definitions

**lines**

The number of lines to be displayed on the terminal emulation screen for the current session. Values may range from 10 to 150.

**columns**

The number of columns to be displayed for each line. One column is the same width as a single text character. Values may range from 20 to 150.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>lines</td>
<td>24</td>
</tr>
<tr>
<td>columns</td>
<td>80</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The number of lines and columns set with this command controls the screen size when the switch is editing or viewing a text file with the `vi` or `tftp` commands.

- The values set with this command do not control the CLI screen when the switch is operating in normal mode.

- This command can also be used on the secondary CMM.

### Examples

```
-> tty 10 60
```

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

**show tty**
Displays current TTY settings.

**MIB Objects**

```plaintext
systemServices
  systemServicesTtyLines
  systemServicesTtyColumns
```
show tty

Displays current TTY settings.

show tty

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Shows the settings made with the tty command.
- This command can also be used on the secondary CMM.

Examples

-> show tty
lines = 24, columns = 80

Release History

Release 7.1.1; command introduced.

Related Commands

tty Specifies the number of TTY lines and columns to be displayed.

MIB Objects

systemServices
  systemServicesTtyLines
  systemServicesTtyColumns
tftp

Starts a TFTP client session that enables a file transfer to an TFTP server.

\texttt{tftp [options] host [port]}

**Syntax Definitions**

- \textit{options} Enter a question mark (?) to get a list of options.
- \textit{host} Specifies the IP address of the TFTP server.
- \textit{port} Specifies the port for the TFTP transfer.

**Defaults**

- If a path is not specified with the filename, the current path is used by default (for example, /flash).
- If a local filename is not specified, the remote filename is used by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The OmniSwitch supports TFTP client functionality only.
- A TFTP server has no provisions for user authentication.
- When downloading a file to the switch, the file size must not exceed the available flash space.

**Examples**

\texttt{-> tftp -g -l local_file -r remote_file 198.51.100.100}

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- \texttt{cd} Changes the current working directory of the switch.
- \texttt{pwd} Displays the current working directory of the switch.
- \texttt{ls} Displays the contents of a specified directory or the current working directory.

**MIB Objects**
N/A
sftp

Starts an SFTP session. An SFTP session provides a secure file transfer method.

`sftp [options] {ip_address}`

### Syntax Definitions

**options**

Enter a question mark (?) to get a list of options.

**ip_address**

Specifies the IPv4 or IPv6 address for the SFTP session.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- You must have a valid username and a password for the specified host.
- After logging in, SFTP commands are supported. Some of these commands are defined in the following table:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cd path</code></td>
<td>Change remote path to ‘path’.</td>
</tr>
<tr>
<td><code>lcd path</code></td>
<td>Change local directory to ‘path’.</td>
</tr>
<tr>
<td><code>chmod mode path</code></td>
<td>Change permissions of file ‘path’ to ‘mode’.</td>
</tr>
<tr>
<td><code>help</code></td>
<td>Display command help information.</td>
</tr>
<tr>
<td><code>get remote-path [local path]</code></td>
<td>Download a file from the remote path to the local path.</td>
</tr>
<tr>
<td><code>lls [path]</code></td>
<td>Display local directory listing.</td>
</tr>
<tr>
<td><code>ln oldpath newpath</code></td>
<td>Creates a symbolic link (symlink) to the remote file.</td>
</tr>
<tr>
<td><code>symlink oldpath newpath</code></td>
<td>Creates a symbolic link (symlink) to the remote file.</td>
</tr>
<tr>
<td><code>mkdir path</code></td>
<td>Create local directory.</td>
</tr>
<tr>
<td><code>lpwd</code></td>
<td>Print local working directory.</td>
</tr>
<tr>
<td><code>ls [path]</code></td>
<td>Display remote directory listing.</td>
</tr>
<tr>
<td><code>mkdir path</code></td>
<td>Create remote directory.</td>
</tr>
</tbody>
</table>
### Examples

```
-> sftp 12.251.11.122
login as:
-> sftp
       [-o ssh_option] [-P sftp_server_path] [-R num_requests]
       [-S program] [-s subsystem | sftp_server] host
       sftp [[user@]host[:file [file]]]
sftp [[user@]host[:dir[/]]]
sftp -b batchfile [user@]host
```

### Release History

Release 7.1.1; command was introduced.

### Related Commands

- **ftp**: Starts an FTP session.
- **ssh**: Invokes Secure Shell on the switch. Secure Shell is used to make a secured connection to a remote system or device.

### MIB Objects

**SystemServices**

- `systemServicesArg1`
- `systemServicesAction`
ftp

Starts an FTP session.

\texttt{ftp \{port [default | service\_port] | admin-state [enable | disable] | ip\_address\} [vrf name] ftp admin-state [enable | disable]}

\textbf{Syntax Definitions}

- \textit{name} The name of the VRF.
- \textit{default} Sets the port back to the default of 21.
- \textit{service\_port} The TCP service port number. Must be 21 or between between 20000-20999.
- \textit{enable | disable} Enables or disables FTP access.
- \textit{ip\_address} Specifies the IPv4 address for the FTP session.

\textbf{Defaults}

N/A

\textbf{Platforms Supported}

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\textbf{Usage Guidelines}

- You must have a valid username and password for the specified host.
- The default FTP directory is /\texttt{flash}.

\textbf{Examples}

- \texttt{-> ftp port 20000}
- \texttt{-> ftp admin-state disable}
- \texttt{-> ftp 172.17.6.228}
- \texttt{-> vrf vrf1 ftp admin-state enable}

\textbf{Release History}

Release 7.1.1; command introduced.
Release 7.3.1; \textit{vrf} parameter added.
Related Commands

- **cd**: Changes the current working directory of the switch.
- **pwd**: Displays the current working directory of the switch.
- **ls**: Displays the contents of a specified directory or the current working directory.

MIB Objects

- systemServices
  - systemServicesArg1
  - systemServicesAction
  - alaIpFtpAdminStatus
show ftp

Displays the current FTP server settings like the port used for FTP, the FTP server's status in the given VRF.

[vrf name] show ftp

Syntax Definitions

name The name of the VRF.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show ftp
Ftp Admin-State = Enabled
Ftp Port = 21

Release History

Release 7.1.1; command introduced.
Release 7.3.1; vrf parameter added.

Related Commands

ftp Starts an FTP session.

MIB Objects

alaIpFtpAdminStatus
alaIpFtpPort
The switch can be configured and monitored using WebView, which is a web-based device management tool. Web Management CLI commands allow you to enable/disable web-based management and configure certain WebView parameters, such as Secure Socket Layer (SSL).

MIB information for the Web Management commands is as follows:

Filename: ALCATEL-INDI-WEBMGT-MIB.mib
Module: alcatelINDIWebMgtMIB

A summary of the available commands is listed here:

```
webview server
webview access
webview force-ssl
webview http-port
webview https-port
webview ssl-strong-ciphers
webview wlan cluster-virtual-ip precedence
webview wlan cluster-virtual-ip
show webview
show webview wlan config
```
webview server

Enables or disables the web management server on the switch.

[vrf name] webview server {enable | disable}

Syntax Definitions

name
  The name of the VRF.

enable
  Enables the web management server on the switch.

disable
  Disables the web management server on the switch.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebView Server</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- If the WebView Server is disabled, WebView Access is automatically disabled.
- VRF name must either be ‘default’ or pre-defined VRF (user-defined).

Examples

-> webview server enable
-> webview server disable
-> vrf vrf1 webview server enable

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; vrf parameter added.
Related Commands

webview access  Enables/disables WebView access on the switch.
show webview  Displays web management configuration information.

MIB Objects

alaIND1WebMgtConfigMIBGroup
  alaInd1WebMgtServerStatus
**webview access**

Enables or disables web management access on the switch.

```bash
[vrf name] webview access {enable | disable}
```

### Syntax Definitions

- **name**: The name of the VRF.
- **enable**: Enables the web management access on the switch.
- **disable**: Disables the web management access on the switch.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebView Access</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>6900 X48C4E/V48C8/C32E/T24C2</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- If Web Access is enabled, the WebView Server is automatically enabled.
- VRF name must either be ‘default’ or pre-defined VRF (user-defined).

### Examples

```bash
-> webview access enable
-> webview access disable
-> vrf vrf1 webview access enable
```

### Release History

Release 7.1.1; command was introduced.
Release 7.3.1; `vrf` parameter added.
Related Commands

- **webview server**  Enables/disables the web server on the switch.
- **show webview**  Displays web management configuration information.

MIB Objects

alaIND1WebMgtConfigMIBGroup
  alaInd1WebMgtAdminStatus
**webview force-ssl**

Enables or Disables Force SSL on the switch. SSL is a protocol that establishes and maintains secure communication between SSL-enabled servers and clients.

`webview force-ssl {enable | disable}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force SSL</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The switch contains a self-signed certificate that may prompt a certificate warning.

**Examples**

`-> webview force-ssl enable`
`-> webview force-ssl disable`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `webview access` Enables/disables WebView access on the switch.
- `show webview` Displays web management configuration information.

**MIB Objects**

- `alaIND1WebMgtConfigMIBGroup`
webview force-ssl
webview http-port

Changes the port number for the embedded web management server.

`webview http-port {default | port port}`

---

**Syntax Definitions**

- **default**
  Restores the port to its default (80) value.

- **port**
  The desired port number for the embedded Web server. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>80</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

|  6360 |  6465 |  6560 |  6570M |  6860 |  6860N |  6865 |  6900 |  6900 | 6900 X48C6/T48C6/ |  9900 |
|-------|-------|-------|--------|-------|--------|-------|-------|-------| X48C4E/V48C8/ |       |
|       |       |       |        |       |        |       |       |       | C32E/T24C2/ |       |
|       |       |       |        |       |        |       |       |       | X24C2      |       |
| Yes   | Yes   | Yes   | Yes    | Yes   | Yes    | Yes   | Yes   | Yes   | Yes        | Yes   |

---

**Usage Guidelines**

All WebView sessions must be terminated before entering this command.

---

**Examples**

- `-> webview http-port port 1025`
- `-> webview http-port default`

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**webview access**  Enables/disables WebView access on the switch.
**show webview**  Displays web management configuration information.

MIB Objects

alaIND1WebMgtConfigMIBGroup
- alaIND1WebMgtHttpPort
webview https-port

Changes the default secure (HTTPS) port for the embedded web management server.

```
webview https-port {default | port port}
```

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Restores the port to its default (443) value.</td>
<td>The desired HTTPS port number. The number must be in the range 0 to 65535; well-known port numbers cannot be configured.</td>
</tr>
<tr>
<td>port</td>
<td>443</td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>443</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

All WebView sessions must be terminated before entering this command.

**Examples**

```
-> webview https-port port 1026
-> webview https https-port default
```

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **webview access**: Enables/disables WebView access on the switch.
- **show webview**: Displays web management configuration information.

**MIB Objects**

- **alaIND1WebMgtConfigMIBGroup**
  - **alaIND1WebMgtHttpsPort**
webview ssl-strong-ciphers

Enables or disables support of only SSL strong cipher algorithms in order to prevent client opening connections to the switch using weak algorithms.

webview ssl-strong-ciphers {enable | disable}

---

**Syntax Definitions**

| enable | Enables the strong cipher requirement. |
|disable | Disables the strong cipher requirement. |

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/N48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (X48C6/T48C6/)</td>
<td>Yes (X48C4E/N48C8/)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When enabled the following algorithms will not be supported: RC4-SHA, RC4-MD5, ECDHE-RSA-RC4-SHA, IDEA-CBC-SHA, DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, ECDHE-RSA-DES-CBC3-SHA, aNULL, eNULL, EXPORT, DES, MD5, PSK, RC4.

**Examples**

- > webview ssl-strong-ciphers enable
- > webview ssl-strong-ciphers disable

**Release History**

Release 8.4.1.R02; command was introduced.

**Related Commands**

- **webview access** Enables/disables WebView access on the switch.
- **show webview** Displays web management configuration information.

**MIB Objects**

alaIND1WebMgtConfigMIBGroup
Web Management Commands

webview ssl-strong-ciphers
**webview wlan cluster-virtual-ip precedence**

Sets the preference for obtaining the cluster virtual IP address for WebView re-direct. The WLAN cluster virtual IP address can be obtained from LLDP or configured manually. The precedence allows to set the preference between the LLDP and manual configuration in case when both are available.

**webview wlan cluster-virtual-ip precedence {lldp | configured}**

### Syntax Definitions

- **lldp**
  - The preference to obtain the WLAN cluster virtual IP address is set to LLDP.

- **configured**
  - The preference to obtain the WLAN cluster virtual IP address is set to the manually configured WLAN cluster virtual IP address.

### Defaults

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldp</td>
<td>configured</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use this command to set the preference for obtaining the cluster virtual IP address for WebView re-direct.

- If more than one cluster virtual IP address is obtained through LLDP on the same port, the recently obtained IP is considered.

- If more than one cluster virtual IP is obtained through LLDP on different ports, the recently obtained IP is considered.

- If the precedence is set for LLDP obtained IP address, but there is no LLDP obtained cluster virtual IP address, then the manually configured cluster virtual IP address will be considered if configured.

- If the precedence is set for manually configured cluster virtual IP address, but there is no configured IP address present, then the LLDP obtained cluster virtual IP address will be considered if received.

### Examples

- `-> webview wlan cluster-virtual-ip precedence lldp`
- `-> webview wlan cluster-virtual-ip precedence configured`
**Release History**

Release 8.4.1 R02; command was introduced.

**Related Commands**

`show webview wlan config`  
Displays the AP cluster virtual IP configured on the switch.

**MIB Objects**

`alaIND1WebMgtWlanIpPrecedence`
**webview wlan cluster-virtual-ip**

Configures the cluster virtual IP address of the Access Point (AP) in the switch. The WebView server on the switch redirects the URL to the AP (Virtual IP Address) URL when the WLAN Management is accessed from WebView.

**webview wlan cluster-virtual-ip**  
*virtual-ip-address-of-wlan-cluster*

---

**Syntax Definitions**

```
virtual-ip-address-of-wlan-cluster  Virtual IP address (IPV4) of the AP cluster.
```

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Model</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to configure the AP cluster virtual IP address to access the OAW-AP web interface from the WebView.

**Examples**

```
-> webview wlan cluster-virtual-ip 10.25.6.8
```

**Release History**

Release 8.4.1 R02; command was introduced.

**Related Commands**

- **show webview wlan config**  
  Displays the AP cluster virtual IP configured on the switch.

**MIB Objects**

```
alaIND1WebMgtWlanConfiguredIpAddress
```
**show webview wlan config**

Displays the cluster virtual IP precedence configuration, WLAN AP cluster virtual IP configured on the switch, and WLAN AP cluster virtual IP obtained through LLDP.

```
show webview wlan config
```

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show webview wlan config
WebView WLAN Cluster-Virtual-IP Precedence = LLDP
WebView WLAN Cluster-Virtual-IP configured address = 0.0.0.0
WebView WLAN Cluster-Virtual-IP LLDP address = 1.1.1.1
```

**output definitions**

- **WebView WLAN Cluster-Virtual-IP Precedence**: The precedence set for obtaining the cluster virtual IP address of the AP.
- **WebView WLAN Cluster-Virtual-IP configured address**: The manually configured cluster virtual IP address.
- **WebView WLAN Cluster-Virtual-IP LLDP address**: The cluster virtual IP address obtained from the LLDP packets.

**Release History**

Release 8.4.1R02; command was introduced.
Related Commands

**webview wlan cluster-virtual-ip precedence**
Allows to set the preference for the choice of cluster virtual IP address for WebView re-direct.

**webview wlan cluster-virtual-ip**
Configures the virtual IP address of the Access Point (AP) clusters in the switch.

MIB Objects

alaIND1WebMgtWlanIpPrecedence
alaIND1WebMgtWlanConfiguredIpAddressType
alaIND1WebMgtWlanConfiguredIpAddress
alaIND1WebMgtWlanLldpIpAddressType
alaIND1WebMgtWlanLldpIpAddress
**show webview**

Displays web management configuration information.

```
[vrf name] show webview
```

### Syntax Definitions

- **name**: The name of the VRF.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If a VRF name is specified, the enabled/disabled state for WebView Server and WebView Access for the specified VRF is displayed.

### Examples

```
-> show webview

WebView Server = Enabled
WebView Access = Enabled
WebView Force-SSL = Enabled
WebView HTTPS-Port = 443
WebView SSL-Strong-Ciphers = Enabled
WebView TLS Version = 1.2
```

```
vrf1:-> show webview

WebView Server = Enabled,
WebView Access = Enabled,
WebView Force-SSL = Enabled,
WebView HTTPS-Port = 443
WebView SSL-Strong-Ciphers = Enabled
```

### Output Definitions

- **WebView Server**: Indicates whether web management server is enabled or disabled.
- **WebView Access**: Indicates whether web management access is enabled or disabled.
output definitions (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force SSL</td>
<td>Indicates whether Force SSL is enabled or disabled. If this is enabled, it means that SSL is forced on an HTTP session and hence HTTPS protocol is negotiated between the client and server.</td>
</tr>
<tr>
<td>Web Management Https Port</td>
<td>The port configured for a secure HTTP connection (SSL enabled).</td>
</tr>
<tr>
<td>Web SSL-Strong-Ciphers</td>
<td>Indicates whether SSL strong cipher requirement is enabled or disabled.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 7.3.1; vrf parameter added.

Related Commands

webview server
webview access
webview force-ssl
webview ssl-strong-ciphers

Enables/disables web management server on the switch.

Enables/disables Webview access on the switch.

Enables/disables SSL on the switch.

Enables/disables SSL strong ciphers on the switch.

MIB Objects

alaIND1WebMgtConfigMIBGroup
alaInd1WebMgtServerStatus
alaInd1WebMgtAdminStatus
alaInd1WebMgtSsl
alaInd1WebMgtHttpsPort
alaInd1WebMgtSSLSStrongCiphers
The Configuration Manager feature allows you to configure your switch using an ASCII-based text file. CLI commands may be typed into a text document—referred to as a configuration file—and then uploaded and applied to the switch.

MIB information for the Configuration Manager commands is as follows:

- **Filename:** ALCATEL-IND1-CONFIG-MGR-MIB.mib
- **Module:** alcatelIND1ConfigMgrMIB

A summary of the available commands is listed here:

```
configuration apply
configuration error-file-limit
show configuration status
configuration cancel
configuration syntax-check
configuration snapshot
show configuration snapshot
write terminal
configuration apply network-sync
```
configuration apply

Applies a configuration file to the switch. Files may be applied immediately or after a designated timer session. With the timer session option, files are applied either at a scheduled date and time or after a specified period of time (i.e., a countdown) has passed.

```
configuration apply filename [at hh:mm month dd [year]] | [in hh:mm] [verbose]
```

### Syntax Definitions

- **filename**
  
  The name of the configuration text file to be applied to the switch (e.g., `newfile1`).

- **at hh:mm**
  
  Designates a timer session in which a configuration file is applied at a specified date and time in the future. Values for `hh` range from 00 through 23. Values for `mm` range from 00 through 59. Values for `dd` range from 01 through 31. Values for month range from january through december. The switch assumes either the current year or the next calendar year for month and day pairs that precede the current date.

- **{dd month | month dd} [year]**
  
  Designates a timer session in which the configuration file is applied after a specific amount of time (i.e., a countdown) has passed. Values for `hh` range from 00 through 23. Values for `mm` range from 00–59.

- **in hh:mm**
  
  Designates a timer session in which the configuration file is applied at a specified date and time in the future. Values for `hh` range from 00 through 23. Values for `mm` range from 00 through 59.

- **verbose**
  
  When verbose is entered, information is displayed on your workstation’s console as each command in the configuration file is applied.

### Defaults

By default, `verbose` error checking is not performed.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- The `configuration apply` command only applies settings to the running configuration. The `boot.cfg` file does not get overwritten.

- It is recommended that you check all configuration files for syntax errors before applying them to your switch.

- To schedule a timer session in which a file is applied at a specific date and time, enter `at` followed by the hour, minute, month, day, and year. The switch assumes either the current calendar year or the next calendar year for dates beginning January 1.
To schedule a timer session in which a file is applied after a specific amount of time (i.e., a countdown) has passed, enter `in` followed by the number of hours and minutes.

Verbose mode is not supported for timer sessions.

The keyword, `authkey`, along with a related alpha-numeric text string, are automatically included in many snapshot files (e.g., `configuration snapshot all`). The text string following the `authkey` keyword represents a login password that has been encrypted twice. (The first encryption occurs when a password is first created by a user; the second encryption occurs when a configuration snapshot is taken.) This dual encryption further enhances switch security. However, it is important to note that any configuration file (including a generated snapshot) that includes this dual-encrypted password information will result in an error whenever it is applied to the switch via the `configuration apply` command. This is a valid switch function and does not represent a significant problem. If an `authkey`-related error is the only error detected, simply remove all `authkey`-related syntax using a text editor. If a new password is required for the switch, include valid password syntax in the configuration file or immediately issue a new password by using the `password` command at the command prompt. For more information on passwords, refer to page 39-65.

Examples

```
-> configuration apply new_configuration at 12:00 15 november
-> configuration apply new_configuration at 12:00 november 15
-> configuration apply newfile1 in 01:30
-> configuration apply my_switch_config in 00:05
-> configuration apply asc.1.snap in 23:00
-> configuration apply aaa_config in 12
-> configuration apply vlan_config verbose
-> configuration apply vlan_config
...```

Note. When the `configuration apply` command is entered without `at` or `in` syntax information, one or more dots “.” is displayed in the next line, immediately following the command line. This indicates command progress; each dot represents 256 text lines in the configuration file processed by the configuration apply mechanism.

Release History

Release 7.1.1; command was introduced.

Related Commands

`configuration syntax-check`  Performs a syntax and authorization check of all CLI commands contained in a configuration file.

MIB Objects

```
alcatelIND1ConfigMgrMIBObjects
  configFileName
  configFileMode
  configFileAction
  configTimerFileName
  configTimerFileTime
```
configuration error-file-limit

Specifies the maximum number of configuration error files allowed in the switch’s /flash directory. Error files are normally generated when a configuration file is applied to the switch. Error files are identified by their .err extension. When the maximum number of .err files is exceeded, any new error file will overwrite the .err file with the oldest timestamp.

configuration error-file-limit number

Syntax Definitions

number

Indicate the number of error files allowed in the /flash directory. The valid range is from 1 to 25 files.

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>1</td>
</tr>
</tbody>
</table>

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When the error file limit is set to 1 (the default value), the next error file generated by the switch will replace the existing one.
- When the error file limit is set to a value greater than 1, when a new error file that exceeds the maximum limit is created, the switch will automatically remove the error file with the smallest timestamp.
- The error files generated by the switch have the .err extension.
- If you want to save an error file, you may change the file name so that it does not have the .err extension, or you can move it from the /flash directory.

Examples

-> configuration error-file-limit 2
-> configuration error-file-limit 1

Release History

Release 7.1.1; command was introduced.
Related Commands

configuration apply  
Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.

configuration cancel  
Cancels a pending timer session for a configuration file.

MIB Objects

alcatelIND1ConfigMgrMIBobjects  
configErrorFileMaximum
show configuration status

Displays whether there is a pending timer session scheduled for a configuration file and indicates whether the running configuration and the saved configuration files are identical or different. This command also displays the number of error files that will be held in the flash directory.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6</th>
<th>6900X48C4E/V48C8</th>
<th>9900X24C2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- A timer session can be scheduled using the configuration apply command. For more information, refer to page 64-2.
- The screen output File configuration </path/filename>: scheduled at dd/mm hh:mm indicates that a timer session has been scheduled for a later time.
- The output No file configuration has been scheduled indicates an idle timer session (i.e., no timer session has been scheduled for a configuration file).
- The output File configuration is in progress indicates that a file is currently being applied to the switch.
- The output File configuration </path/filename>: completed with 2 errors indicates that the named file was applied to the switch with two recorded errors.
- When the running and saved configurations are the same, the output Running configuration and saved configuration are identical will be displayed.
- When the running and saved configurations are the different, the output Running configuration and saved configuration are different will be displayed.
- To synchronize the running and saved configuration, use the write memory command.
Examples

`-> show configuration status`

Release History

Release 7.1.1; command was introduced.

Related Commands

- `configuration apply` Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
- `configuration cancel` Cancels a pending timer session for a configuration file.
- `configuration error-file-limit` Specifies the maximum number of configuration error files allowed in the switch’s `/flash` directory.
- `write memory` Copies the running configuration (RAM) to the working directory.

MIB Objects

- configTimerFileGroup
  - configTimerFileStatus
configuration cancel

Cancels a pending timer session for a configuration file.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes/C4E/V48C8/C32E/T24C2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> configuration cancel

Release History

Release 7.1.1; command was introduced.

Related Commands

configuration apply Applications a configuration file to the switch. Also used for scheduling a timer session for a configuration file.

show configuration status Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

configTimerFileGroup
configTimerClear
**configuration syntax-check**

Performs a syntax and authorization check of all CLI commands contained in a configuration file.

`configuration syntax-check path/filename [verbose]`

**Syntax Definitions**

- **path/filename**: The configuration file being checked for syntax and authorization errors. If a configuration file is located in another directory, be sure to specify the full path. For example, `/flash/working/asc.1.snap`.

- **verbose**: When `verbose` is specified in the command line, all syntax contained in the configuration file is printed to the console, even if no error is detected. When `verbose` is not specified in the command line, cursory information (number of errors and error log file name) will be printed to the console only if a syntax or configuration error is detected.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>6360</td>
<td>Yes</td>
</tr>
<tr>
<td>6465</td>
<td>Yes</td>
</tr>
<tr>
<td>6560</td>
<td>Yes</td>
</tr>
<tr>
<td>6570M</td>
<td>Yes</td>
</tr>
<tr>
<td>6860</td>
<td>Yes</td>
</tr>
<tr>
<td>6860N</td>
<td>Yes</td>
</tr>
<tr>
<td>6865</td>
<td>Yes</td>
</tr>
<tr>
<td>6900</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 V72/C32</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
</tr>
<tr>
<td>9900</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When an error is detected, an error file (.err) is automatically generated by the switch. By default, this file is placed in the root `/flash` directory. To view the contents of a generated error file, use the `view` command. For example, `view asc.1.snap.1.err`.

- The syntax, `mac alloc`, is automatically included in many snapshot files (e.g., `configuration snapshot all`). All `mac alloc`-related syntax is valid during switch boot up only (i.e., it cannot be applied while the switch is in run-time operation). Because snapshot files are commonly used as configuration files, syntax checks may detect `mac alloc` syntax and issue an error (along with a generated .err file). This is a valid switch function and does not represent a significant problem. If a `mac alloc`-related error is the only error detected, simply remove the syntax using a text editor, then re-check the file using the `configuration syntax-check` command.

- It is recommended that you check all configuration files for syntax errors before applying them to your switch.
Examples

-> configuration syntax-check vlan_file1
  ..

Note. When the configuration syntax-check command is entered, one or more dots “.” is displayed in the command output. This indicates command progress; each dot represents 256 text lines in the configuration file processed by the syntax check mechanism.

Release History

Release 7.1.1; command was introduced.

Related Commands

configuration apply  Applies a configuration file to the switch. Also used for scheduling a timer session for a configuration file.
show configuration status  Displays whether there is a pending timer session scheduled for a configuration file.

MIB Objects

configFileGroup
  configFileGroupName
  configErrorFileName
  configErrorFileMaximum
  configFileManager
  configFileStatus
configuration snapshot

Generates a snapshot file of the switch’s non-default current running configuration. A snapshot can be generated for all current network features or for one or more specific network features. A snapshot is a single text file that can be viewed, edited, and reused as a configuration file.

configuration snapshot [feature_list | all] [path/filename]

Syntax Definitions

feature_list
The description for the network feature(s) to be included in the snapshot. You may enter more than one network feature in the command line. Enter a question mark (?) on the command line to get a list of features (configuration snapshot ?).

all
Includes all network features in the snapshot.

path/filename
A user-defined name for the resulting snapshot file. For example, test_snmp_snap. You may also enter a specific path for the resulting file. For example, the syntax /flash/working/test_snmp_snap places the test_snmp_snap file in the switch’s /flash/working directory.

Defaults

If a file name is not specified, the default file name asc.#.snap is used. Here, # indicates the order in which the default file is generated. For example, the first default file name to be generated is asc.1.snap, the second default file name to be generated is named asc.2.snap, etc. By default, all snapshot files are placed in the root /flash directory.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Only current, non-default configuration settings are written to the snapshot file.
- You may enter more than one network feature in the command line. Separate each network feature with a space and no comma. Network features may be entered in any order.
- The snapshot file is automatically placed in the root /flash directory unless otherwise specified.

Examples

- -> configuration snapshot all
- -> configuration snapshot qos health aggregation new_file1
- -> configuration snapshot snmp_snapshot snmp
-> configuration snapshot 802.1q
-> configuration snapshot ?

ZEROCONF WEBMGT VRRP VM-SNOOPING VLAN VIRTUAL-CHASSIS
VFC VCSP UDLD TEST-OAM SYSTEM SVCMDR STP SPB-ISIS
SNMP SLB SIP SESSION SECURITY SAA RIPNG RIP QOS QMR
PVLAN PTP PPPOE-IA PORT-MAPPING PORT-MANAGER POLICY
PMM OSPF3 OSPF OPENFLOW NTP MRP MVRP
MODULE MGMT-AGENT MACSEC LOOPBACK-TEST
LOOPBACK-DETECTION LLDP LINKAGG
LINK-FAULT-PROPAGATION LDP LANPOWER ISIS
IPV6-UDPRELAY IPV6 IPSEC IPMS IPMR IP-Routing
IP-DHCP-RELAY IP INTERFACE HEALTH HA-VLAN FCoE EVB
ETHERNET-OAM ERP EFM-OAM DHL DHCPV6-SNOOPING
DHCPV6-SERVER DHCPV6-RELAY DHCP-SNOOPING DHCP-SERVER
DHCP-MESSAGE-SERVICE DHCP-ACTIVE-LEASE-SERVICE
DEVICE-PROFILE DA-UNP CLOUD-AGENT CHASSIS CAPABILITY
BRIDGE BGP BFD AUTO-FABRIC APP-MONITORING
APP-FINGERPRINT ALL ALARM-MANAGER AAA

Release History
Release 7.1.1; command was introduced.

Related Commands
show configuration snapshot  Displays the switch’s current running configuration.

MIB Objects
configManager
  configSnapshotFileName
  configSnapshotAction
  configSnapshotAllSelect
show configuration snapshot

Displays the switch’s current running configuration for all features or for the specified feature(s).

show configuration snapshot [feature_list]

Syntax Definitions

feature_list Specify the feature(s) for which you want to display the running configuration. List the features separated by a space with no comma. Enter a question mark (?) on the command line to get a list of features (show configuration snapshot ?).

Defaults

By default, this command shows configuration information for all features.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

• Use this command to view the current configuration for any feature shown in the table.
• Configurations are listed below the name of each feature.
• Features with no current configuration show only the name of the feature.

Examples

-> show configuration snapshot
-> show configuration snapshot aaa bridge
  ! Bridging :

  ! AAA :
  aaa authentication default "local"
  aaa authentication console "local"
  user "public" read All write All no auth authkey 391b0e74dbd13973d703ccea4a8e30

-> show configuration snapshot ?
  <cr> ZEROCONF WEBMGT VRRP VM-SNOOPING VLAN
  VIRTUAL-CHASSIS VFC VCSP UDLL TEST-OAM SYSTEM
  SVCGR STP SPF-ISIS SNMP SLB SIP SESSION
  SECURITY SAA RIPNG RIP QOS QMR VLAN PTP
  PPPOE-IA PORT-MAPPING PORT-MANAGER POLICY PNM
OSPF3 OSPF OPENFLOW NTP MRP MVRP
MODULE MGMT-AGENT MACSEC LOOPBACK-TEST
LOOPBACK-DETECTION LLDP LINKAGG
LINK-FAULT-PROPAGATION LDP LANPOWER ISIS
IPV6-UDPRELAY IPV6 IPSEC IPMS IPMR IP-Routing
IP-DHCP-RELAY IP INTERFACE HEALTH HA-VLAN FCOE
EVB ETHERNET-OAM ERP EFM-OAM DHL DHCPV6-SNOOPING
DHCPV6-SERVER DHCPV6-RELAY DHCP-SNOOPING
DHCP-SERVER DHCP-MESSAGE-SERVICE
DHCP-ACTIVE-LEASE-SERVICE DEVICE-PROFILE DA-UNP
CLOUD-AGENT CHASSIS CAPABILITY BRIDGE BGP BFD
AUTO-FABRIC APP-MONITORING APP-FINGERPRINT ALL
ALARM-MANAGER AAA

Release History

Release 7.1.1; command was introduced.

Related Commands

write terminal Displays the switch’s current running configuration for all features.

MIB Objects

configManager
  configSnapshotFileName
  configSnapshotAction
  configSnapshotAllSelect
write terminal

Displays the switch’s current running configuration for all features.

write terminal

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>V72/C32</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6900 X48C6/T48C6/X48C4E/V48C8/C32E/T24C2/X24C2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Configurations are listed below the name of each feature.
- Features with no current configuration show only the name of the feature.

Examples

- write terminal

Release History

Release 7.1.1; command was introduced.

Related Commands

show configuration snapshot Displays the switch’s current running configuration for all features or for the specified feature(s).

MIB Objects

configManager

    mib_configSnapshotAllSelect
**configuration backup restore**

Allows to backup or restore the user custom configuration in the `/flash` directory.

```
configuration {backup | restore}
```

**Syntax Definitions**

- **backup**: Backups the user custom configuration (session banner, user table and `vcboot.cfg`) in the `/flash` directory.
- **restore**: Restores the user custom configuration in the `/flash` directory.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>Platform</th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- When backup option is issued, the session banner file, the `vcboot.cfg` of the current running directory and all the `userTable` files are collected and stored in a single tar file (sing tar file) in "'/flash/config-recovery" folder.
- When restore option is issued, the backup file is extracted and restored to the current running directory. The switch must be reloaded for the restored files to be applied.
- The backup option can be issued multiple times. However only 10 backup occurrences will be stored in the recovery folder. Post the 10th occurrence the first occurrence is deleted to save the current backup file.

**Examples**

```
-> configuration backup
-> configuration restore
```

**Release History**

Release 8.7 R2; command was introduced.
Related Commands

N/A

MIB Objects

configFileRecovery
configuration apply network-sync

Performs pre-provisioning or runtime network level synchronization for AOS Micro Services (AMS) using the publisher/subscriber model.

configuration apply network-sync filename [community community-name | local-apply]

Syntax Definitions

filename The name of the file with the AOS configuration to be synchronized.
community-name Performs synchronization only on switches with the corresponding community name.
local-apply Apply the configuration to the local switch.

Defaults

N/A

Platforms Supported

Not supported in this release.

Usage Guidelines

- Use the configuration syntax-check command to validate the configuration file syntax before network synchronization.
- It is recommended to have only global, and not local, level switch configuration information propagated for network level configurations.
- The file name “preprovision.txt” is a pre-defined name used for pre-provisioning purposes. Pre-provisioning applies only to new nodes that join the network, the configuration will not be applied to existing nodes. Refer to the AMS section of the Switch Management Guide for additional information.

Examples

-> configuration apply network-sync preprovision.txt
-> configuration apply network-sync adaptive-test

Release History

Release 8.6R1; command not supported.

Related Commands

configuration syntax-check Performs a syntax and authorization check of all CLI commands contained in a configuration file.

MIB Objects

N/A
SNMP Commands

This chapter includes descriptions for Trap Manager and SNMP Agent commands. The commands are used for configuring SNMP settings on the switch.

- SNMP station commands can create, modify, or delete an SNMP station. Also included is a show command for monitoring current SNMP station status.

- SNMP trap commands configure SNMP trap settings. Traps can be replayed and filtered. Also, test traps can be generated to verify that individual traps are being correctly handled by the Network Management Station (NMS). The SNMP trap commands set includes show commands for monitoring SNMP trap information.

- SNMP agent commands configure SNMP security levels on the switch. Also includes show commands for monitoring the current SNMP security status.

MIB information for SNMP Community commands is as follows:

- **Filename**: SNMP-COMMUNITY-MIB.mib
- **Module**: snmpCommunityMIB

MIB information for Trap Manager commands is as follows:

- **Filename**: ALCATEL-IND1-TRAP-MGR-MIB.mib
- **Module**: alcatelIND1TrapMgrMIB

MIB information for SNMP Agent commands is as follows:

- **Filename**: ALCATEL-IND1-SNMP-AGENT-MIB.mib
- **Module**: alcatelIND1SNMPAgentMIB
A summary of the available commands is listed here:

| SNMP station commands       | snmp station             |
|                            | show snmp station        |
| SNMP engine ID commands     | snmp snmp-engineid-type  |
|                            | show snmp snmp-engineid  |
| SNMP community map commands | snmp community-map       |
|                            | snmp community-map mode  |
|                            | show snmp community-map  |
| SNMP security commands      | snmp security            |
|                            | snmp security tsm        |
|                            | snmp tsm-map             |
|                            | show snmp tsm-map        |
|                            | show snmp security       |
|                            | show snmp statistics     |
|                            | show snmp mib-family     |
| SNMP trap commands          | snmp-trap absorption     |
|                            | snmp-trap to-webview     |
|                            | snmp-trap replay-ip      |
|                            | snmp-trap filter-ip      |
|                            | snmp authentication-trap |
|                            | show snmp-trap replay-ip |
|                            | show snmp-trap filter-ip |
|                            | show snmp authentication-trap |
|                            | show snmp-trap config    |
| Event commands              | event-action             |
|                            | show event-action        |
### snmp station

Adds a new SNMP station; modifies or deletes an existing SNMP station.

```
snmp station {ip_address | ipv6_address | domain_name} {[port] [username] [v1 | v2 | v3 | v3 tsm local-identity local_string remote-identity remote_string] [enable | disable]}
```

```
no snmp station {ip_address | ipv6_address | domain_name}
```

#### Syntax Definitions

- **ip_address**: The IP address to which SNMP unicast traps will be sent.
- **ipv6_address**: The IPv6 address to which SNMP unicast traps will be sent.
- **domain_name**: A Fully Qualified Domain Name (FQDN) to which SNMP unicast traps will be sent. Specify a domain name up to 255 characters in length.
- **port**: A UDP or TLSTCP destination port.
- **username**: The user name on the switch or external server used to send traps to the SNMP station(s). The username specified here must match an existing user account name.
- **v1**: Specifies that traps are sent using SNMP version 1.
- **v2**: Specifies that traps are sent using SNMP version 2.
- **v3**: Specifies that traps are sent using SNMP version 3.
- **tsm**: The TSM security model for SNMP. The security model can be selected only for SNMP version 3.
- **local_string**: The file name of the local certificate. To be configured when TSM mode is selected.
- **remote_string**: The file name of the remote certificate. To be configured when TSM mode is selected.
- **enable**: Enables the specified SNMP station.
- **disable**: Disables the specified SNMP station.

#### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port</strong></td>
<td>162 (for UDP)</td>
</tr>
<tr>
<td></td>
<td>10162 (for TLSTCP)</td>
</tr>
<tr>
<td>**v1</td>
<td>v2</td>
</tr>
<tr>
<td>**enable</td>
<td>disable**</td>
</tr>
</tbody>
</table>
### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>6900 V72/C32</td>
<td>6900 X48C6/T48C6/</td>
<td>6900 C32E/T24C2/</td>
<td>6900 X24C2</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the **no** form of the command to remove an existing SNMP station.
- When adding an SNMP station, specify an IP address or FQDN **plus username parameters**. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 username1** is a valid command entry.
- A maximum of 50 SNMP sessions can be established in the switch.
- When modifying an SNMP station, specify an IP address or FQDN **plus at least one additional parameter**. For example, the syntax **snmp station 1.2.3.4** is not a valid command entry; however, **snmp station 1.2.3.4 v2** is a valid command entry.
- When an FQDN is specified with this command, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.
- When the SNMP station is enabled, the switch transmits traps to the specified IP or IPv6 address.
- For UDP the default port 162 is commonly used for traps; however, the destination port can be redefined to accommodate an SNMP station using a nonstandard port. The destination port specified must correspond with the UDP destination port configured at the receiving SNMP station(s).
- For TLSTCP the default port 10162 is commonly used for traps; however, the destination port can be redefined to accommodate an SNMP station using a nonstandard port. The destination port specified must correspond with the TLSTCP destination port configured at the receiving SNMP station(s).
- To send SNMP traps over TLS connection, the SNMP station needs to be configured with TSM user along with certificate identities.
- The local_identity and remote_identity are the names of certificate file. If the contents of local or remote certificates are changed, the updated certificates must be manually copied from master or primary to all secondaries and slaves. A reboot is required for the changes to be applied.
- When TSM security model is enabled, all the v1/v2/v3 USM requests and traps are discarded.
- When TSM security model is disabled, all v1/v2/v3 (USM and TSM) requests and traps are allowed.
- In TSM security model SNMP requests are supported over IPv4 transport only.

### Examples

```bash
-> snmp station 168.22.2.111 username2 v1 disable
-> snmp station 168.151.2.101 "test lab"
-> snmp station 170.1.2.3 username1 enable
-> snmp station 1.1.2.2 v2
-> no snmp station 2.2.2.2
```
- snmp station 300::1 enable
- no snmp station 300::1

- snmp station upam.omnivista.com username2 v1 disable
- snmp station upam.omnivista.com v2
- no snmp station upam.omnivista.com
- snmp station opendaylight.com enable v2 public
  ERROR: DNS lookup failed, unknown host opendaylight.com
- snmp station 168.22.1.1 joe v3 tsm local-identity aluSubagent.crt
  remote-identity manager.crt enable

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R1; *domain_name* parameter option added.
Release 8.6R1; *tsm*, *local-identity*, and *remote-identity* parameters added.

**Related Commands**

*show snmp station* Displays the current SNMP station information.

**MIB Objects**

*trapStationTable*
  - trapStationIP
  - trapStationPort
  - trapStationUser
  - trapStationProtocol
  - trapStationRowStatus

*alaTrapInetStationTable*
  - alaTrapInetStationIPType
  - alaTrapInetStationIP
  - alaTrapInetStationPort
  - alaTrapInetStationRowStatus
  - alaTrapInetStationProtocol
  - alaTrapInetStationUser
  - alaTrapInetStationSecurityModel
  - alaTrapInetStationLocalIdentity
  - alaTrapInetStationRemoteIdentity
**show snmp station**

Displays the current SNMP station status and details.

**show snmp station [details]**

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

|----|-----:|-----:|-----:|------:|-----:|------:|-----:|-----:|-------------:|-------------------------------------:|-----:|
| Yes|     |     |     |       |      |       |      |     |             |                                     |      |

**Usage Guidelines**

N/A

**Examples**

`-> show snmp station`

```
ipAddress/Port status protocol user
-------------------------------------------------------------
199.199.100.200/8010 enable v3 NMSuserV3MD5DES
199.199.101.201/111 disable v2 NMSuserV3MD5
199.199.102.202/8002 enable v1 NMSuserV3SHADES
199.199.103.203/8003 enable v3 NMSuserV3SHADES
199.199.104.204/8004 enable v3 NMSuserV3SHA
```

`-> show snmp station details`

```
ipAddress/port: 10.255.24.59/162, status: disable, protocol: v2, user: public,
```

```
ipAddress/port: 135.115.207.36/162, status: disable, protocol: v2, user: public,
```

```
ipAddress/port: localhost/10162, status: disable, protocol: v3, security model: tsm,
```
user:            joecool,
local identity:  aluSubagent.crt,
remote identity: manager.crt,
ipAddress/port:  10.255.24.57/162,
status:          enable,
protocol:        v1,
user:            public,

output definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IpAddress</td>
<td>IP Address of the SNMP management station.</td>
</tr>
<tr>
<td>Port</td>
<td>Trap station port number (UDP, TLSTCP).</td>
</tr>
<tr>
<td>status</td>
<td>The Enabled/Disabled status of the SNMP management station.</td>
</tr>
<tr>
<td>protocol</td>
<td>The version of SNMP set for this management station.</td>
</tr>
<tr>
<td>security model</td>
<td>Displays the security model selected.</td>
</tr>
<tr>
<td>user</td>
<td>The user account name.</td>
</tr>
<tr>
<td>local identity</td>
<td>File name of local certificate used, TSM only. This is</td>
</tr>
<tr>
<td></td>
<td>displayed only for SNMP version 3.</td>
</tr>
<tr>
<td>remote identity</td>
<td>File name of remote certificate used, TSM only. This is</td>
</tr>
<tr>
<td></td>
<td>displayed only for SNMP version 3.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; details parameter and local identity, remote identity, and security model output fields added.

Related Commands

snmp station    Adds a new SNMP station; modifies or deletes an existing SNMP station.

MIB Objects

trapStationTable
  trapStationIP
  trapStationPort
  trapStationUser
  trapStationProtocol
  trapStationRowStatus
alaTrapInetStationTable
  alaTrapInetStationIPType
  alaTrapInetStationIP
  alaTrapInetStationPort
  alaTrapInetStationRowStatus
  alaTrapInetStationProtocol
  alaTrapInetStationUser
  alaTrapInetStationLocalIdentity
  alaTrapInetStationRemoteIdentity
**snmp snmp-engineid-type**

Configures a unique engine ID for the OmniSwitch SNMP agent.

```
snmp snmp-engineid-type {text | mac-address | ipv4-address | ipv6-address} snmp-engineid
{text_string | mac_address | ipv4_address | ipv6_address}
```

```
snmp snmp-engineid-type mac-address snmp-engineid default
```

### Syntax Definitions

- **text_string**: A text string that will be converted to a hexadecimal value. The valid range is 1–27 characters.
- **mac_address**: A specific MAC Address (for example, 00:00:39:59:f1:0c).
- **ipv4_address**: An IPv4 address that will be converted to a hexadecimal value.
- **ipv6_address**: An IPv6 address that will be converted to a hexadecimal value.

### Defaults

By default, the SNMP engine ID is set to the base MAC address for the switch appended to the enterprise value for OmniSwitch platforms (for example, if the enterprise value is “8000195603” and the switch base MAC address is “2c:fa:a2:13:e4:02”, then the default engine ID is set to “80001956032cfaa213e402”).

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- To set the engine ID back to the default value, specify the **mac-address** parameter and the **default** parameter with this command. For example, `snmp snmp-engineid-type mac-address snmp-engineid default`.

- Note that the **snmp-engineid** keyword is entered after the parameter that specifies the type of engine ID format to use and before the actual value that matches the specified parameter type. For example, if the **ipv4-address** parameter is specified, enter the IPv4 address value after the **snmp-engineid** keyword (`snmp snmp-engineid-type ipv4-address snmp-engineid 10.2.2.1`).

- When a text string, an IPv4 address, or an IPv6 address is specified, the value is automatically converted to a hexadecimal value that is then appended to the OmniSwitch enterprise value to form the SNMP engine ID for the switch.

### Examples

```
-> snmp snmp-engineid-type text snmp-engineid "test lab"
```
```plaintext
-> snmp snmp-engineid-type mac-address snmp-engineid 00:2a:95:01:02:03
-> snmp snmp-engineid-type ipv4-address snmp-engineid 168.22.2.2 111
-> snmp snmp-engineid-type mac-address snmp-engineid default
```

**Release History**

Release 8.3.1.R02; command was introduced.

**Related Commands**

- `show snmp snmp-engineid` Displays the current SNMP engine ID information.

**MIB Objects**

- `snmpAgtEngineIdType`
- `snmpAgtEngineId`
show snmp snmp-engineid

Displays the current SNMP engine ID value for the switch.

show snmp snmp-engineid

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release History</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guideline**

N/A

**Examples**

```bash
-> show snmp snmp-engineid
snmp engineId type       snmp engineId
-------------------+--------------------------------
default Mac           80001956032cfaa213e402
```

**output definitions**

<table>
<thead>
<tr>
<th>snmp engineId type</th>
<th>The type of engine ID (default Mac, Text, Ipv4, or Ipv6).</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp engineId</td>
<td>The SNMP engine ID value that uniquely identifies the OmniSwitch SNMP agent. This value is comprised of the OmniSwitch enterprise ID plus the configured SNMP engine ID value, in hexadecimal format.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.3.1.R02; command was introduced.
Related Commands

**snmp snmp-engineid-type**

Configures the type and value of the SNMP engine ID for the switch.

MIB Objects

- **snmpAgtEngineIdType**
- **snmpAgtEngineId**
**snmp community-map**

Configures and enables a community string on the switch and maps it to an existing user account name.

```plaintext
snmp community-map {
  [hash-key string | community_string] user useraccount_name
} [enable | disable]
```

no snmp community-map community_string

**Syntax Definitions**

- **hash-key string**: The hashed format of a community string.
- **community_string**: A community string in the form of a text string. This string must be between 1 and 32 characters.
- **useraccount_name**: A user name in the form of a text string. This name must match a user login account name already configured on the switch or configured remotely on an external AAA server. This user name must be between 1 and 32 characters.
- **enable**: Enables SNMP community string mapping.
- **disable**: Disables SNMP community string mapping.

**Defaults**

By default, SNMP community map authentication is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Community strings are stored in a hashed format in the `show configuration snapshot snmp` output. To view community string mappings in plain-text use the `show snmp community-map` command.
- Community strings configured on the switch are used for v1 and v2c SNMP managers only.
- The user account name must be a current user account recognized by the switch. For a list of current user names use the `show user` command. To create a new user account, use the `user` command.
- There is one to one mapping between each community string and a user account name.
- Privileges attached to the community string are the ones inherited from the user account name that created it.
- The community-map mode must be enabled and the community string carried over each incoming v1 or v2c SNMP request must be mapped to a user account name in order to be processed by the SNMP agent.

**Examples**

- snmp community-map community1 user testname1
- snmp community-map community1 enable

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `snmp community-map mode` Enables the local community strings database.

**MIB Objects**

SNMPCommunityTable
- snmpCommunityIndex
- snmpCommunitySecurityName
- snmpCommunityStatus
**snmp community-map mode**

Enables the local community strings database.

`snmp community-map mode {enable | disable}`

---

**Syntax Definitions**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables SNMP community map database.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables SNMP community map database.</td>
</tr>
</tbody>
</table>

---

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community mode</td>
<td>disabled</td>
</tr>
</tbody>
</table>

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- The community-map mode must be enabled and the community string carried over each incoming v1 or v2c SNMP request must be mapped to a user account name with SNMP privileges in order to be processed by the SNMP agent.
- When enabled, mapping is contained in the local community strings database populated by using the `snmp community-map` command.

---

**Examples**

```
-> snmp community-map mode enable
-> snmp community-map mode disable
```

---

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**snmp community-map**  Configures and enables a community string on the switch and maps it to an existing user account name.

MIB Objects

```
SNMPCommunityTable
   snmpCommunityIndex
   snmpCommunitySecurityName
   snmpCommunityStatus
```
**show snmp community-map**

Shows the local community strings database.

```bash
show snmp community-map
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guideline

N/A

### Examples

```bash
-> show snmp community-map
Community mode : enabled

status       community string                 user name
-------------+-------------------------------+--------------------------------
enabled       test_string1          bb_usename
enabled       test_string2          rr_usename
disabled      test_string3          cc_usename
disabled      test_string4          jj_usename
```

**output definitions**

- **Status**: The Enabled/Disabled status of the community string.
- **Community String**: The text that defines the community string.
- **User Name**: The user account name.

### Release History

Release 7.1.1; command was introduced.
**Related Commands**

- **snmp community-map**
  Configures and enables a community string on the switch and maps it to an existing user account name.

**MIB Objects**

- N/A
**snmp security**

Configures SNMP security settings.

```
snmp security {no-security | authentication set | authentication all | privacy set | privacy all | trap-only | tls {enable | disable}}
```

### Syntax Definitions

- **no-security**
  
  The switch will accept all SNMP v1, v2, and v3 requests.

- **authentication set**
  
  The switch will accept all requests *except* v1, v2, and non-authenticated v3 set requests. SNMP v1, v2, and non-authenticated v3 set requests will be rejected.

- **authentication all**
  
  The switch will accept all requests *except* v1, v2, and non-authenticated v3 get, get-next, and set requests. SNMP v1, v2, and non-authenticated v3 get, get-next, and set requests will be rejected.

- **privacy set**
  
  The switch will accept *only* authenticated SNMP v3 get, get-next and encrypted v3 set requests. All other requests will be rejected.

- **privacy all**
  
  The switch will accept only encrypted v3 get, get-next, and set requests. All other requests will be rejected.

- **trap-only**
  
  All SNMP get, get-next, and set requests will be rejected.

- **tls enable | disable**
  
  Unblocks (enable) or blocks (disable) the SNMP TLS port 10161.

### Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>privacy all</td>
</tr>
<tr>
<td>tls enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Usage Guidelines

Refer to the table below for a quick-reference list of security parameter and the SNMP request allowances for each parameter.

<table>
<thead>
<tr>
<th></th>
<th>v1 set</th>
<th>v2 set</th>
<th>v3 non-auth set</th>
<th>v1 get</th>
<th>v2 get</th>
<th>v3 non-auth get/next</th>
<th>v3 auth set</th>
<th>v3 auth get/get-next</th>
<th>v3 encryp set</th>
<th>v3 encryp get/get-next</th>
</tr>
</thead>
<tbody>
<tr>
<td>no-security</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
</tr>
<tr>
<td>authentication set</td>
<td>rejected</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
</tr>
<tr>
<td>authentication all</td>
<td>rejected</td>
<td>rejected</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
</tr>
<tr>
<td>privacy set</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
</tr>
<tr>
<td>privacy all</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
<td>accepted</td>
</tr>
<tr>
<td>trap-only</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
<td>rejected</td>
</tr>
</tbody>
</table>

Examples

- `snmp security no-security`
- `snmp security authentication set`
- `snmp security authentication all`
- `snmp security privacy set`
- `snmp security trap-only`

Release History

Release 7.1.1; command was introduced.

Related Commands

`show snmp security` Displays the current SNMP security status.

MIB Objects

`SNMPAgtConfig`

  `SnmpAgtSecurityLevel`
snmp security tsm

Enables or disables TLS encryption for SNMP access.

```bash
snmp security tsm [enable | disable]
```

**Syntax Definitions**

- **enable**: Enables TLS encryption for SNMP access.
- **disable**: Disables TLS encryption for SNMP access.

**Defaults**

By default, the TLS encryption for SNMP access is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The TLS encryption can be enabled only for SNMP version 3.
- In Common Criteria mode (CC mode) TLS encryption for SNMP is enabled by default and cannot be disabled.

**Examples**

```bash
-> snmp security tsm enable
-> snmp security tsm disable
```

**Release History**

Release 8.6R1; command was introduced.

**Related Commands**

- **snmp tsm-map**: Displays the current SNMP security status.

**MIB Objects**

- **SNMPAgtConfig**
  - **snmpAgtTsmAdminState**
**snmp tsm-map**

Allows to map a remote identity or certificate to a user in TSM mode.

```
snmp tsm-map remote-identity remote_string user user_string
```

**Syntax Definitions**

- `remote_string`: File name of remote certificate to be mapped with the user. This string must be between 1 and 128 characters.
- `user_string`: The user name. This string must be between 1 and 32 characters.

**Defaults**

N/A.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The remote identity mapping for user can be done only in TSM mode.
- The remote identity mapping can be done for only one user at a time. It cannot be mapped to multiple users. Mapping it to a different user will replace the existing user.
- If the content of remote certificate is changed, the updated certificate must be manually copied from master or primary to all secondaries and slaves. A reboot is required for the changes to be applied.

**Examples**

```
-> snmp tsm-map remote-identity manager.crt user joe
-> snmp security tsm disable
```

**Release History**

Release 8.6R1; command was introduced.
Related Commands

`show snmp tsm-map` Displays the current SNMP TSM remote identity mapping for a user.

MIB Objects

alaSnmpTsmUserTable
  - alaSnmpTsmUserRemoteIdentity
  - alaSnmpTsmUserName
show snmp tsm-map

Displays the current SNMP TSM remote identity mapping for a user.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

Enter the specific file name of the remote certificate to view the mapping related to it.

Examples

-> show snmp tsm-map
Remote Identity User
-------------------------------------------------------
manager.crt     adam

-> show snmp tsm-map manager.pem
Remote Identity User
-------------------------------------------------------
manager.pem     joecool

output definitions

Remote Identity Displays the file name of the remote certificate mapped to the user.
User Displays the user name mapped to the remote identity.

Release History

Release 8.6R1; command was introduced.
**Related Commands**

- **snmp tsm-map**
  
  Allows to map a remote identity or certificate to a user in TSM mode.

**MIB Objects**

N/A
**show snmp security**

Displays the current SNMP security status.

`show snmp security [tsm]`

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

- Refer to the command on page 65-18 for descriptions of the five SNMP security states: no security, authentication set, authentication all, privacy set, privacy all, and trap only.

- Use the optional parameter `tsm` along with the command to display the configured SNMP TSM status.

**Examples**

```plaintext
-> show snmp security
snmp security = no security

-> show snmp security
snmp security = authentication set

-> show snmp security
snmp security = authentication all

-> show snmp security
snmp security = privacy set

-> show snmp security
snmp security = privacy all

-> show snmp security
snmp security = trap only

-> show snmp security tsm
snmp security tsm = disable
```
output definitions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp security</td>
<td>Displays the configured SNMP security level.</td>
</tr>
<tr>
<td>snmp security tsm</td>
<td>Displays the configured SNMP TLS encryption status.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.
Release 8.6R1; tsm parameter added.

Related Commands

- **snmp security**: Configures the SNMP security settings.
- **snmp security tsm**: Enables or disables TLS encryption for SNMP access.

MIB Objects

N/A
show snmp statistics

Displays the current SNMP statistics.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show snmp statistics
From RFC1907
    snmpInPkts = 801
    snmpOutPkts = 800
    snmpInBadVersions = 0
    snmpInBadCommunityNames = 0
    snmpInBadCommunityUses = 0
    snmpInASNParseErrs = 0
    snmpEnableAuthenTraps = disabled(2)
    snmpSilentDrops = 0
    snmpProxyDrops = 0
    snmpInTooBigs = 0
    snmpOutTooBigs = 0
    snmpInNoSuchNames = 0
    snmpOutNoSuchNames = 0
    snmpInBadValues = 0
    snmpOutBadValues = 0
    snmpInReadOnlys = 0
    snmpOutReadOnlys = 0
    snmpInGenErrs = 0
    snmpOutGenErrs = 0
    snmpInTotalReqVars = 839
    snmpInTotalSetVars = 7
show snmp statistics

```
<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmpInGetRequests</td>
<td>3</td>
</tr>
<tr>
<td>snmpOutGetRequests</td>
<td>0</td>
</tr>
<tr>
<td>snmpInGetNexts</td>
<td>787</td>
</tr>
<tr>
<td>snmpOutGetNexts</td>
<td>0</td>
</tr>
<tr>
<td>snmpInSetRequests</td>
<td>7</td>
</tr>
<tr>
<td>snmpOutSetRequests</td>
<td>0</td>
</tr>
<tr>
<td>snmpInGetResponses</td>
<td>0</td>
</tr>
<tr>
<td>snmpOutGetResponses</td>
<td>798</td>
</tr>
<tr>
<td>snmpInTraps</td>
<td>0</td>
</tr>
<tr>
<td>snmpOutTraps</td>
<td>0</td>
</tr>
</tbody>
</table>
```

From RFC2572

```
<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmpUnknownSecurityModels</td>
<td>0</td>
</tr>
<tr>
<td>snmpInvalidMsgs</td>
<td>0</td>
</tr>
<tr>
<td>snmpUnknownPDUHandlers</td>
<td>0</td>
</tr>
</tbody>
</table>
```

From RFC2573

```
<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmpUnavailableContexts</td>
<td>0</td>
</tr>
<tr>
<td>snmpUnknownContexts</td>
<td>1</td>
</tr>
</tbody>
</table>
```

From RFC2574

```
<table>
<thead>
<tr>
<th>MIB Object</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>usmStatsUnsupportedSecLevels</td>
<td>0</td>
</tr>
<tr>
<td>usmStatsNotInTimeWindows</td>
<td>1</td>
</tr>
<tr>
<td>usmStatsUnknownUserNames</td>
<td>1</td>
</tr>
<tr>
<td>usmStatsUnknownEngineIDs</td>
<td>0</td>
</tr>
<tr>
<td>usmStatsWrongDigests</td>
<td>0</td>
</tr>
<tr>
<td>usmStatsDecryptionErrors</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**output definitions**

<table>
<thead>
<tr>
<th>From RFCxxxx</th>
<th>Displays the RFC number that defines the SNMP MIB objects listed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB Objects</td>
<td>Name of the MIB object listed as an SNMP statistic.</td>
</tr>
<tr>
<td>= (integer)</td>
<td>The number of times the MIB object has been reported to the SNMP management station since the last reset.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `snmp security` Configures the SNMP security settings.

**MIB Objects**

- N/A
**show snmp mib-family**

Displays SNMP MIB information. Information includes MIP ID number, MIB table name, and command family.

`show snmp mib-family [table_name]`

**Syntax Definitions**

`table_name` The name of the MIB table to be displayed.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If a table name is not specified in the command syntax, all MIB table names will be displayed.
- If the command family is not valid for the entire MIB table, the command family will be displayed on a per-object basis.
- Table names are case-sensitive. Therefore, use the exact table names from the MIB database.

**Examples**

```
-> show snmp mib-family trapStationTable
MIP ID  MIB TABLE NAME                                FAMILY
-------+----------------------------------------+---------------------
73733  trapStationTable                      snmp
```

**output definitions**

<table>
<thead>
<tr>
<th>MIP ID</th>
<th>Identification number for the MIP associated with this MIB Table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIB Table Name</td>
<td>Name of the MIB table.</td>
</tr>
<tr>
<td>Family</td>
<td>Command family to which this MIB table belongs.</td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

*show snmp-trap filter-ip*  
Displays the SNMP trap filter information.

**MIB Objects**

N/A
**snmp-trap absorption**

Enables or disables the trap absorption function.

```
snmp-trap absorption {enable | disable}
```

**Syntax Definitions**

- **enable**: Enables SNMP trap absorption. When trap absorption is enabled, identical, repetitive traps sent by applications during a pre-configured time period will be absorbed, and therefore not sent to SNMP Manager stations configured on the switch.

- **disable**: Disables SNMP trap absorption.

**Defaults**

By default, trap absorption is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view the current trap absorption status, use the `show snmp-trap config` command.

**Examples**

```
-> snmp-trap absorption enable
-> snmp-trap absorption disable
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

**show snmp-trap config**  Displays the SNMP trap information. Information includes trap ID numbers and corresponding trap names and families.

MIB Objects

- `trapFilterTable`
- `trapAbsorption`
snmp-trap to-webview

Enables the forwarding of traps to WebView.

```
snmp-trap to-webview {enable | disable}
```

**Syntax Definitions**

- **enable**: Enables WebView forwarding. When WebView forwarding is enabled, all traps sent by switch applications are also forwarded to WebView. This allows a WebView session to retrieve the trap history log.
- **disable**: Disables WebView forwarding.

**Defaults**

By default, WebView forwarding is enabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To view the current WebView forwarding status, use the `show snmp-trap config` command.

**Examples**

- `-> snmp-trap to-webview enable`
- `-> snmp-trap to-webview disable`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- **show snmp-trap config**: Displays the SNMP trap information, including the current status for trap absorption and WebView forwarding.

**MIB Objects**

- `trapFilterTable`  
- `trapToWebView`
**snmp-trap replay-ip**

Replays stored traps from the switch to a specified SNMP station. This command is used to replay (to resend) traps on demand. This is useful in the event when traps are lost in the network.

```
snmp-trap replay-ip {ip_address | ipv6_address | domain_name} [seq_id]
```

### Syntax Definitions

- **ip_address**: The IP address for the SNMP station to which traps will be replayed from the switch.
- **ipv6_address**: The IPv6 address for the SNMP station to which traps will be replayed from the switch.
- **domain_name**: A Fully Qualified Domain Name (FQDN) for the SNMP station to which traps will be replayed. Specify a domain name up to 255 characters in length.
- **seq_id**: The sequence number from which trap replay will begin. Each trap sent by the switch to an SNMP station has a sequence number. The sequence number reflects the order in which the trap was sent to the SNMP station. For example, the first trap sent to an SNMP station has a sequence number of 1; the second trap has a sequence number of 2, etc. If no sequence number is entered, all stored traps are replayed.

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- Use the `show snmp station` command on page 65-6 to display the latest stored sequence number for each SNMP station.
- The switch replays traps in the same order that they were previously sent, beginning from the specified sequence number.
- When traps are replayed, the original dates on which the trap was issued, rather than the current dates are used.
- When an FQDN is specified with this command, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.
snmp-trap replay-ip

- If the specified sequence number is lower than the oldest trap sequence number stored in the switch, the switch replays all stored traps.

- If the specified sequence number is equal to or greater than the oldest trap sequence number stored, the switch replays all stored traps from the specified sequence number up to the latest sequence number.

- If the specified sequence number is greater than the latest sequence number, no traps are replayed.

**Examples**

```
-> snmp-trap replay-ip 172.12.2.100
-> snmp-trap replay-ip 300::1
-> snmp-trap replay-ip upam.omnivista.com
```

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R1; `domain_name` parameter option added.

**Related Commands**

- `show snmp station` Displays the current SNMP station status.
- `show snmp-trap replay-ip` Displays the SNMP trap replay information.

**MIB Objects**

- `trapStationTable`
  - `trapStationReplay`
  - `trapStationNextSeq`
- `alaTrapInetStationTable`
  - `alaTrapInetStationReplay`
  - `alaTrapInetStationNextSeq`
**snmp-trap filter-ip**

Enables or disables SNMP trap filtering. Trap filtering is used to determine whether a trap or group of traps will be sent from the switch to a specified SNMP station.

`snmp-trap filter-ip {ip_address | ipv6_address | domain_name} trap_id_list`

`no snmp-trap filter-ip {ip_address | ipv6_address | domain_name} trap_id_list`

### Syntax Definitions

- **ip_address**
  - The IP address for the SNMP station for which trap filtering is enabled or disabled.

- **ipv6_address**
  - The IPv6 address for the SNMP station for which trap filtering is enabled or disabled.

- **domain_name**
  - A Fully Qualified Domain Name (FQDN) for the SNMP station for which trap filtering is enabled or disabled. Specify a domain name up to 255 characters in length.

- **trap_id_list**
  - Specifies the trap(s) for which filtering is being enabled or disabled. Traps must be specified using the numeric trap ID. You can specify more than one trap in the command line; separate each trap ID with a space and no comma.

### Defaults

By default, SNMP trap filtering is disabled.

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

- To *enable* trap filtering, use the syntax `snmp-trap filter-ip ip_address trap_id_list`.
- To *disable* trap filtering, use the syntax `no snmp-trap filter-ip ip_address trap_id_list`.
- When an FQDN is specified with this command, the switch will resolve the domain name to an IP address. Make sure the domain name maps to a valid and reachable IP address.
- When filtering is enabled, the specified trap(s) *will not* be sent to the SNMP station. When filtering is disabled, the specified traps *will* be sent to the SNMP station.
- To display a list of traps and their ID numbers, use the `show snmp-trap config` command.
**Examples**

-> snmp-trap filter-ip 172.1.2.3 1
-> snmp-trap filter-ip 172.1.2.3 0 1 3 5
-> snmp-trap filter-ip 300::1 1 3 4
-> snmp-trap filter-ip upam.omnivista.com 1 3 5
-> no snmp-trap filter-ip 172.1.2.3 1
-> no snmp-trap filter-ip 172.1.2.3 0 1 3 5
-> no snmp-trap filter-ip 300::1 1 3
-> no snmp-trap filter-ip upam.omnivista.com 1 3 5

**Release History**

Release 7.1.1; command was introduced.
Release 8.5R1; `domain_name` parameter option added.

**Related Commands**

- `show snmp-trap filter-ip` Displays the current SNMP trap filter status.
- `show snmp-trap config` Displays the SNMP trap information, including trap ID numbers, trap names, command families, and absorption rate.

**MIB Objects**

- `trapFilterTable`
  - `trapFilterStatus`
- `alaTrapInetFilterTable`
  - `alaTrapInetFilterStatus`
**snmp authentication-trap**

Enables or disables SNMP authentication failure trap forwarding.

`snmp authentication-trap {enable | disable}`

**Syntax Definitions**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables authentication failure trap forwarding. When enabled, the standard authentication failure trap is sent each time an SNMP authentication failure is detected.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables authentication failure trap forwarding.</td>
</tr>
</tbody>
</table>

**Defaults**

By default, authentication failure trap forwarding is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

- `-> snmp authentication-trap enable`
- `-> snmp authentication-trap disable`

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `show snmp authentication-trap` Displays the current authentication failure trap forwarding status.

**MIB Objects**

- `snmpGroup`
  - `snmpEnableAuthenTraps`
**show snmp-trap replay-ip**

Displays SNMP trap replay information.

```
show snmp-trap replay-ip
```

---

**Syntax Definitions**

N/A

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

N/A

**Examples**

```
-> show snmp-trap replay-ip
ipAddress : oldest replay number
---------------------------------------
199.199.101.200 :       1234
199.199.105.202 :        578
199.199.101.203 :       1638
199.199.101.204 :       2560
upam.omnivista.com:     1849
```

---

**output definitions**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address or Fully Qualified Domain Name (FQDN) of the SNMP station manager that replayed the trap.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Oldest Replay Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of the oldest replayed trap.</td>
<td></td>
</tr>
</tbody>
</table>

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **snmp-trap replay-ip**
  - Replays stored traps from the switch to a specified SNMP station.

MIB Objects

- **trapStationTable**
  - trapStationReplay
  - trapStationNextSeq

- **alaTrapInetStationTable**
  - alaTrapInetStationReplay
  - alaTrapInetStationNextSeq
show snmp-trap filter-ip

Displays the current SNMP trap filter status.

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines
To display a list of traps and their ID numbers, use the `show snmp-trap config` command.

Examples

```
-> show snmp-trap filter-ip
ipAddress       trapId list
-------------------------
199.199.101.200 : 0 1 2 3
199.199.101.201 : no filter
199.199.105.202 : 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
199.199.101.203 : 20 22 30
199.199.101.204 : no filter
upam.omnivista.com : 1 3 5
```

output definitions

<table>
<thead>
<tr>
<th>Output</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAddress</td>
<td>IP address or Fully Qualified Domain Name (FQDN) of the SNMP management station that recorded the traps.</td>
</tr>
<tr>
<td>TrapId List</td>
<td>Identification number for the traps being filtered.</td>
</tr>
</tbody>
</table>

Release History
Release 7.1.1; command was introduced.
Related Commands

- **snmp-trap filter-ip**: Enables or disables SNMP trap filtering.
- **show snmp-trap config**: Displays the SNMP trap information, including trap ID numbers, trap names, command families, and absorption rate.

MIB Objects

- **trapFilterTable**
  - **trapFilterEntry**
- **alaTrapInetFilterTable**
  - **alaTrapInetFilterStatus**
show snmp authentication-trap

Displays the current authentication failure trap forwarding status (i.e., enable or disable).

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show snmp authentication-trap
snmp authentication trap = disable

Release History

Release 7.1.1; command was introduced.

Related Commands

snmp authentication-trap Enables or disables SNMP authentication failure trap forwarding.

MIB Objects

sessionAuthenticationTrap
show snmp-trap config

Displays SNMP trap information. Information includes trap ID numbers, trap names, command families, and absorption rate. This command also displays the Enabled/Disabled status of SNMP absorption and the Traps to WebView service.

```
show snmp-trap config
```

### Syntax Definitions

N/A

### Defaults

N/A

### Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Usage Guidelines

N/A

### Examples

```
-> show snmp-trap config
Absorption service : enabled
Traps to WebView : enabled

<table>
<thead>
<tr>
<th>Id</th>
<th>trapName</th>
<th>family</th>
<th>absorption</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>coldStart</td>
<td>chassis</td>
<td>15 seconds</td>
</tr>
<tr>
<td>1</td>
<td>warmStart</td>
<td>chassis</td>
<td>15 seconds</td>
</tr>
<tr>
<td>2</td>
<td>linkDown</td>
<td>interface</td>
<td>15 seconds</td>
</tr>
<tr>
<td>3</td>
<td>linkUp</td>
<td>interface</td>
<td>15 seconds</td>
</tr>
<tr>
<td>4</td>
<td>authenticationFailure</td>
<td>snmp</td>
<td>15 seconds</td>
</tr>
<tr>
<td>5</td>
<td>entConfigChange</td>
<td>module</td>
<td>15 seconds</td>
</tr>
<tr>
<td>30</td>
<td>slPseudoCAMStatusTrap</td>
<td>bridge</td>
<td>15 seconds</td>
</tr>
<tr>
<td>31</td>
<td>slbTrapException</td>
<td>loadbalancing</td>
<td>15 seconds</td>
</tr>
<tr>
<td>32</td>
<td>slbTrapConfigChanged</td>
<td>loadbalancing</td>
<td>15 seconds</td>
</tr>
<tr>
<td>33</td>
<td>slbTrapOperStatus</td>
<td>loadbalancing</td>
<td>15 seconds</td>
</tr>
<tr>
<td>34</td>
<td>ifMauJabberTrap</td>
<td>interface</td>
<td>15 seconds</td>
</tr>
<tr>
<td>35</td>
<td>sessionAuthenticationTrap</td>
<td>session</td>
<td>15 seconds</td>
</tr>
</tbody>
</table>
```
output definitions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Identification number for the trap.</td>
</tr>
<tr>
<td>Trap Name</td>
<td>Name of the trap.</td>
</tr>
<tr>
<td>Family</td>
<td>Family to which the trap belongs.</td>
</tr>
<tr>
<td>Absorption</td>
<td>Time needed for the trap to process.</td>
</tr>
</tbody>
</table>

Release History

Release 7.1.1; command was introduced.

Related Commands

- **show snmp mib-family** Displays SNMP MIB information.
- **snmp-trap absorption** Enables or disables the trap absorption function.
- **snmp-trap to-webview** Enables or disables the forwarding of SNMP traps to WebView.

MIB Objects

- **trapConfigTable**
  - **trapConfigEntry**
event-action

Triggers the specified script to run when the specified event occurs.

```
event-action {trap trigger_string script script_string | script-time-limit num}

no event-action trap name
```

**Syntax Definitions**

- `trigger_string`: The name of the trigger. In the case of a trap, this is the trap name.
- `script_string`: The path and the name of the script to run.
- `num`: The maximum amount of time a script can run (30-600).
- `name`: The name of the trap to remove the event from.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>script-time-limit</td>
<td>60 seconds.</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>V72/C32</td>
<td></td>
<td></td>
<td></td>
<td>X48C6/T48C6/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X48C4E/V48C8/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C32E/T24C2/</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X24C2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- If the prefix for the script is not `/flash/python`, the path will be assumed to be under that directory.
- Each event can only be assigned a single script but a script can be assigned to multiple events.
- Only users that have write privileges for the AAA partition management family can create scripts in the `/flash/python` directory.
- The `show snmp-trap config` command can be used to view the list of traps available on the switch.

**Examples**

```
-> event-action trap linkDown script /flash/python/link_event.py
-> event-action trap stpNewRoot script stp_event.py
```

**Release History**

Release 7.3.4; command was introduced.
Related Commands

show event-action  Shows the scripts and statistics associated with the events.

MIB Objects

alaEventActionTable
  alaEventActionType
  alaEventActionName
  alaEventActionScriptName
  alaEventActionRowStatus
show event-action

Displays the scripts and statistics associated with the events.

```
show event-action [statistics | trap name [statistics]]
```

Syntax Definitions

- **name**
  - The name of the trap to display statistics for.
- **statistics**
  - Displays the statistics for all configured events or a specific trap.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

In the case of a virtual-chassis, the event-script can be run independently on the Master or Slave chassis. The Master and slave chassis have separate launch counters and the script launch counter will not be synchronized across chassis.

Examples

```
-> show event-action

<table>
<thead>
<tr>
<th>type</th>
<th>name</th>
<th>script</th>
</tr>
</thead>
<tbody>
<tr>
<td>trap</td>
<td>linkDown</td>
<td>link_event.py</td>
</tr>
<tr>
<td>trap</td>
<td>stpNewRoot</td>
<td>stp_event.py</td>
</tr>
<tr>
<td>trap</td>
<td>sessionAuthenticationTrap</td>
<td>catchAll.py</td>
</tr>
</tbody>
</table>

-> show event-action statistics

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Script</th>
<th>Last Launched</th>
<th>Launch Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>trap</td>
<td>linkDown</td>
<td></td>
<td>2014-10-23 13:45:34</td>
<td>2</td>
</tr>
</tbody>
</table>

output definitions

- **Type**
  - The type of event trigger.
- **Name**
  - The name of the event. In the case of a trap, this is the trap name.
- **Script**
  - The name and location of the script associated with the event.
SNMP Commands

Output Definitions (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script Last Launched</td>
<td>The date and time the script was last run.</td>
</tr>
<tr>
<td>Launch Count</td>
<td>The number of times the script has been launched by the event.</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command was introduced.

Related Commands

event-action

This command will cause the specified script to be run when the specified event occurs.

MIB Objects

alaEventActionTable
  alaEventActionType
  alaEventActionName
  alaEventActionScriptName
OmniVista Cirrus is a network management solution to deliver zero touch provisioning using cloud.

OmniVista Cirrus solution provides reduced costs, ease of devices provisioning and a unified wired/wireless management from the cloud. The solution also provides an ability to identify each device uniquely and provide a freemium/premium solution based on the user policy.

Deployment of OmniVista Cirrus provides easy to use management and monitoring tools in a network and the ability to manage the network using devices ranging from workstations to smart phones.

MIB information for the OmniVista Cirrus commands is as follows:

<table>
<thead>
<tr>
<th>Filename:</th>
<th>ALCATEL-IND1-SYSTEM-MIB.mib</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module:</td>
<td>alcatelIND1SystemMIB</td>
</tr>
</tbody>
</table>

A summary of the available commands is listed here.

```
cloud-agent admin-state
cloud-agent discovery-interval
cloud-agent remove-inconsistent-certificate
show cloud-agent status
show cloud-agent vpn status
naas license call-home interval
naas license apply file
show naas license
show naas-agent status
```
cloud-agent admin-state

Enables or disables OmniVista Cirrus functionality globally for the switch.

`cloud-agent admin-state {enable | disable | disable force | restart}`

Syntax Definitions

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables OmniVista Cirrus for the switch.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables OmniVista Cirrus for the switch.</td>
</tr>
<tr>
<td>disable force</td>
<td>Disables OmniVista Cirrus for the switch and disconnects from the VPN.</td>
</tr>
<tr>
<td>restart</td>
<td>Restart option implicitly triggers “disable force” followed by “enabled”.</td>
</tr>
</tbody>
</table>

Defaults

By default, OmniVista Cirrus is globally enabled for the switch.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- OmniVista Cirrus is globally enabled for the switch only when the switch boots up without a configuration file [vcboot.cfg] or the configuration file size is zero bytes.

- If the switch boots up with a configuration file, the feature is enabled only if the administrative state of OmniVista Cirrus is explicitly enabled using the `cloud-agent admin-state` command. Hence, the default value is disabled in this case.

- The switch must have access to the DHCP server in the customer network with zero configurations on the devices.

- If the OmniVista Cirrus administrative state is disabled at run-time, it will take effect only after a reboot.

- If the OmniVista Cirrus administrative state is enabled at run-time, it will immediately trigger call-home with the activation server, if a connection was not established prior to that.

- When the OmniVista Cirrus administrative state is disabled at run-time while the connection is in progress or established, it will not have any consequences on the switch. If `write memory` is issued, the switch will not call-home even if the switch reboots or has a takeover. However, if the discovery interval timer is running, the next call-home will be terminated.
• The restart option implicitly triggers the administrative states of disable force followed by enabled. This will enable a user to restart call-home from OmniVista Cirrus.

• If the switch is in an intermediate state (downloading an image from image server, pre-provisioning, write memory, flash syncro, call-home, etc.), the cloud agent admin state disable force will display an error message: “OV Cloud agent is in progress. Please retry after some time.”

**Examples**

-> cloud-agent admin-state enable
-> cloud-agent admin-state disable

**Release History**

Release 8.4.1 R03; command introduced.
Release 8.5R1; restart parameter added.

**Related Commands**

*cloud-agent discovery-interval* Configures the time interval after which the switch will call-home the activation server, in case of any fatal error.

*show cloud-agent status* Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

**MIB Objects**

*ovCloudAgent*
  
  ovCloudAgentAdminState
cloud-agent discovery-interval

Configures the time interval after which the switch will call-home to the activation server, in case of any error.

cloud-agent discovery-interval minutes

Syntax Definitions

minutes The time interval to call-home after an error. The valid range is 2-3600 minutes.

Defaults

By default, the discovery interval is set to 30 minutes.

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Call-home with the activation server will be immediately triggered when OmniVista Cirrus administrative state is enabled at run-time, if a connection was not established prior to that.

- When the OmniVista Cirrus administrative state is disabled at run-time while the connection is in progress or in an established connection, it will not have any consequences on the switch. If write memory is issued, the switch will not call-home even if the switch reboots or has a takeover. However, if the discovery interval timer is running, the next call home will be terminated.

- When trying to connect to the openVPN server, if the connection is not established in 90 seconds, the switch will move to an error state and will call home after the expiry of the discovery interval.

Examples

- -> cloud-agent discovery-interval 60
- -> cloud-agent discovery-interval 90

Release History

Release 8.4.1 R03; command introduced.
Related Commands

- **cloud-agent admin-state**: Enables or disables OmniVista Cirrus functionality globally for the switch.
- **show cloud-agent status**: Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

MIB Objects

- `ovCloudAgent`
  - `ovCloudAgentDiscoveryInterval`
cloud-agent remove-inconsistent-certificate

Removes the certificate received from the OmniVista Activation server on all units in the VC, if the certificate status is inconsistent.

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900 V72/C32</th>
<th>6900 X48C6/T48C6/</th>
<th>6900 X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>6900 X48C4E/T24C2/</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- When this command is issued, a warning is generated: "This command may render the switch incapable of connecting with OV-Cloud if not used with caution. Confirm (Y/N)."

- If accepted by pressing (Y) and the certificate status is not inconsistent, an error message is displayed: “Certificate status is Consistent. Cannot delete certificate.” The existing OmniVista Cirrus agent state machine will not be interrupted.

Examples

-> cloud-agent remove-inconsistent-certificate

Release History

Release 8.5R1; command introduced.
Related Commands

cloud-agent admin-state
Enables or disables OmniVista Cirrus functionality globally for the switch.

show cloud-agent status
Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

MIB Objects

ovCloudAgent

ovCloudAgentRemoveInconsistentCertificate
show cloud-agent status

Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

**show cloud-agent status**

---

**Syntax Definitions**

N/A

---

**Defaults**

N/A

---

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The command **show cloud-agent status** will be valid only if call-home is enabled. Else, only the default values, if present, will be displayed.

- DHCP address, DHCP IP address mask, Gateway, Activation URL, Proxy URL, Proxy IP will be displayed based on the DHCP response parameters received.

- DNS server, DNS domain will be displayed with the current DNS configuration in the switch, if call-home is enabled.

**Examples**

```
-> show cloud-agent status
Admin State                     : Enabled,
Activation Server State         : completeOK,
Device State                    : DeviceManaged,
Error State                     : None,
Cloud Group                     : pmrb98earnoc10,
DHCP Address                    : 135.254.171.88,
DHCP IP Address Mask            : 255.255.255.0,
Gateway                         : 135.254.171.1,
Activation Server               : activation.myovcloud.com:443,
NTP Server                       : 135.254.171.160,
DNS Server                       : 10.67.0.254,
DNS Domain                      : netaos.in,
Proxy Server                     : 192.168.70.226:8000,
VPN Server                      : pmrb98earnoc10.tenant.vpn.dev.myovcloud.com:443,
Preprovision Server             : pmrb98earnoc10.tenant.ovd.dev.myovcloud.com:80,
```
OmniVista Cirrus Commands

show cloud-agent status

OV tenant                       : pingram999.ov.dev.ovcirrus.com:443,
VPN DPD Time (sec)              : 0,
Image Server                   : -, Image Download Retry Count : -,
Discovery Interval (min)        : 30,
Time to next Call Home (sec)    : -, Call Home Timer Status : Not-Running,
Discovery Retry Count           : 1
Certificate Status              : Consistent

Release History

Release 8.4.1 R03; command introduced.
Release 8.5R1; “Certificate Status” added in command display.

Related Commands

cloud-agent admin-state     Enables or disables OmniVista Cirrus functionality globally for the
                              switch.
show cloud-agent vpn status  Displays the OmniVista Cirrus VPN status.

MIB Objects

ovCloudAgent
  ovCloudAgentAdminState
  ovCloudAgentDiscoveryInterval
  ovCloudAgentDeviceState
  ovCloudAgentTimeToNextCallhome
show cloud-agent vpn status

Displays the OmniVista Cirrus VPN status.

Examples

-> show cloud-agent vpn status
  VPN status                : Connected,
  VPN Assigned IP           : 10.8.0.4,
  VPN DPD time (sec)        : 600

output definitions

VPN Status               Refers to OmniVista Cirrus VPN status. The various VPN states are:
                        • Connecting—OpenVPN’s initial state
                        • Wait—Waiting for initial response from server
                        • Auth—Authenticating with server
                        • Get_Config—Downloading configuration options from server
                        • Assign_IP—Assigning IP address to virtual network interface
                        • Add_Routes—Adding routes to system
                        • Connected—Initialization sequence completed
                        • Reconnecting—A restart has occurred
                        • Exiting—A graceful exit is in progress

VPN Assigned IP          Displays the VPN server assigned IP for the VPN connection towards
                          the OmniVista Cirrus.

VPN DPD time (sec)       Displays the VPN Dead Peer Detection (DPD) time value in seconds.
**Release History**
Release 8.4.1 R03; command introduced.

**Related Commands**
- `cloud-agent admin-state` Enables or disables OmniVista Cirrus functionality globally for the switch.
- `show cloud-agent status` Displays the OmniVista Cirrus status and parameters received from the DHCP and activation server.

**MIB Objects**
- `ovCloudAgent`
  - `ovCloudAgentDeviceState`
  - `ovCloudAgentVpnStatus`
naas license call-home interval

Configures the time interval for on-demand call-home to ALE License Activation Server instead of waiting for the next call-home interval.

naas license call-home interval \{minutes | now\}

**Syntax Definitions**

- **minutes**
  The time interval to call-home to ALE License Activation Server. The valid range is 0-1440 minutes.

- **now**
  Specify "now" or "1" minute interval parameter for the call-home to start immediately without waiting for the already set time interval.

**Defaults**

By default, the call-home interval is set to 30 minutes.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Call-home with the ALE License Activation Server will be immediately triggered, when this command is applied on the switch.
- The call-home to the ALE License Activation Server will be continuous after this command is applied.
- On specifying the now parameter or 1 minute interval, call-home starts immediately without waiting for the already set time interval.
- If the call-home interval is set to “0” and device is in CAPEX undecided state, the NaaS call home will be disabled.
- The configured call-home interval can be modified or overridden by the ALE License Activation Server response later.

**Examples**

- `-> naas license call-home interval 60`
- `-> naas license call-home interval now`

**Release History**

Release 8.8R1; command introduced.
Related Commands

**show naas-agent status**
Displays the status and parameters received from the DHCP and ALE License Activation Server.

**show naas license**
Displays all information related to NaaS license received from the ALE License Activation Server.

MIB Objects

`alaNaasConfig`

`alaNaasConfigCallhomeInterval`
**naas license apply file**

Activates the NaaS license on the switch.

`naas license apply file_name`

---

**Syntax Definitions**

`file_name` The name of the license file containing the license keys.

**Defaults**

NaaS Essential License is the base license enabled by default.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Installs the license manually in case of no internet connection or to recover the switch from degraded state.
- The NaaS Essential License is the base License enabled by default on the OmniSwitch.

**Examples**

`-> naas license apply file licenseFile.v2c`

**Release History**

Release 8.8R1; command introduced.

**Related Commands**

- `show naas-agent status` Displays the status and parameters received from the DHCP and ALE License Activation Server.
- `show naas license` Displays all information related to NaaS license received from the ALE License Activation Server.

**MIB Objects**

`alaNaasConfig`

`alaNaasConfigLicenseFile`
show naas license

Displays all information related to NaaS license received from the ALE License Activation Server.

show naas license

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Use this command to verify NaaS licenses installed on the switch.
- The default NaaS Essential License is the base AOS Software enabled by default. Advanced license includes DC and 10G license.

Examples

-> show naas license

VC Serial Device Device Call-home Grace Valid Start/End Expiry
Number Mode State Period Period Licenses Day Time
---+------------------+---------+-----------+-----------+--------+-------------+--------+-----------------+
1  V2980734 NAAS Licensed 30         N/A     Essential N/A         N/A
1  V2980734 NAAS Licensed 30         N/A     Advanced N/A         N/A
1  V2980734 NAAS Licensed 30 30 Management 30/08/2022 273 day(s)
1  V2980734 NAAS Licensed 30 0 Upgrade 30/08/2022 273 day(s)
**output definitions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC</td>
<td>Displays the virtual chassis identifier.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Displays the serial number of the switch</td>
</tr>
<tr>
<td>Device Mode</td>
<td>Displays the device mode. (CAPEX, CAPEX-UNDECIDED, NAAS, UNKNOWN)</td>
</tr>
<tr>
<td>Device State</td>
<td>Displays the device state. (LICENSED, GRACE, DEGRADED)</td>
</tr>
<tr>
<td>Call-home Period</td>
<td>Displays the time interval to call-home to ALE License Activation Server.</td>
</tr>
<tr>
<td>Grace Period</td>
<td>Displays the time remaining for the switch to go into degraded mode. In grace period, switch can be managed but not upgraded.</td>
</tr>
<tr>
<td>Valid Licenses</td>
<td>Displays the information on Naas license installed on the switch. (Essential, Management, Upgrade)</td>
</tr>
<tr>
<td>Start/End Day</td>
<td>Displays the validity of the license with reference to serial number of the switch.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Displays the time left for the switch to go into degraded mode or or days until the subscription expires.</td>
</tr>
</tbody>
</table>

**Release History**

Release 8.8R1; command introduced.

**Related Commands**

- **show naas-agent status**
  
  Displays the status and parameters received from the DHCP and ALE License Activation Server.

- **naas license apply file**
  
  Activates the Naas license on the switch.

**MIB Objects**

N/A
show naas-agent status

Displays the status and parameters received from the DHCP and ALE License Activation Server.

show naas-agent status

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use this command to verify ALE License Activation Server information on the switch.

Examples

-> show naas-agent status
Proxy Server : N/A,
Activation Server : license.ovng.myovcloud.com,
DNS Server : 8.8.8.8,
DNS Domain : omnivista.com,
NTP Server : 216.239.35.12,
Call Home Timer Status : Not-Running,

Release History

Release 8.8R1; command introduced.
**Related Commands**

- `naas license apply file` Activates the NaaS license on the switch.
- `show naas license` Displays all information related to NaaS license received from the ALE License Activation Server.

**MIB Objects**

N/A
67 OpenFlow Commands

OpenFlow is a communications interface defined between the control and forwarding layers that is used in a Software Defined Network (SDN). OpenFlow separates the control plane and the data plane in the switch. Traditionally, switches and routers have made decisions on where packets should travel based on rules local to the device. With OpenFlow, only the data plane exists on the switch itself, and all control decisions are communicated to the switch from a central Controller. The OmniSwitch can operate in AOS or OpenFlow mode, including a modified OpenFlow mode known as Hybrid mode.

MIB information for the Web Management commands is as follows:

- **Filename:** ALCATEL-IND1-OPENFLOW-MIB.mib
- **Module:** alcatelIND1OpenflowMIB

A summary of the available commands is listed here:

<table>
<thead>
<tr>
<th>OpenFlow Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>openflow back-off-max</td>
</tr>
<tr>
<td>openflow idle-probe-timeout</td>
</tr>
<tr>
<td>openflow logical-switch</td>
</tr>
<tr>
<td>openflow logical-switch controller</td>
</tr>
<tr>
<td>openflow logical-switch interfaces</td>
</tr>
<tr>
<td>show openflow</td>
</tr>
<tr>
<td>show openflow logical-switch</td>
</tr>
</tbody>
</table>
**openflow back-off-max**

Configures the maximum amount of time to wait between Controller connection attempts.

```
openflow back-off-max seconds
```

**Syntax Definitions**

```
seconds
```

The back-off-max value, in seconds. The valid range is from 0 - 60.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>60</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If set to 0, setting is disabled.

**Examples**

```
-> openflow back-off-max 0
-> openflow back-off-max 32
-> openflow back-off-max 60
```

**Release History**

Release 7.3.4; command introduced

**Related Commands**

`show openflow` Displays global OpenFlow configuration parameters.

**MIB Objects**

```
alaOpenflowGlobalMIBConfigObjects
alaOpenflowGlobalBackoffMax
```

openflow idle-probe-timeout

Configures the idle probe timeout value.

openflow idle-probe-timeout seconds

---

Syntax Definitions

seconds The idle probe timeout value, in seconds. The valid range is 1 - 60.

---

Defaults

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>15</td>
</tr>
</tbody>
</table>

---

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

---

Usage Guidelines

If set to 0, idle probing is disabled.

---

Examples

- -> openflow idle-probe-timeout 0
- -> openflow idle-probe-timeout 15
- -> openflow idle-probe-timeout 60

---

Release History

Release 7.3.4; command introduced

---

Related Commands

show openflow Displays global OpenFlow configuration parameters.

---

MIB Objects

alaOpenflowGlobalMIBConfigObjects
alaOpenflowGlobalIdleProbeTimeout
openflow logical-switch

Configures an OpenFlow Logical Switch. An OpenFlow Logical Switch consists of a portion of the switch's resources that are managed by an OpenFlow Controller (or set of Controllers) via the OpenFlow Agent.

**openflow logical-switch name** [probe-time num | failure-detect-time num | tcp-buffer-size num | dpid string] [admin-state {enable | disable}] [mode {normal | api | pfc-channel}] [version {1.0 | 1.3.1}+] [learned-mac-update {enable | disable}] [vlan vlan_id] [table-miss-action {drop | controller}]

**no openflow logical-switch <name>**

### Syntax Definitions

- **name**
  The Logical Switch name (up to 32 characters).

- **probe-time num**
  Configures probe-time for a logical switch in the pfc-channel mode which will override the existing global idle-probe-time for sending echo-requests to the OpenFlow Controller. (1-60)

- **failure-detect-time num**
  Configures the failure-detect-time for a logical switch in the pfc-channel mode for detecting a disconnection to the OpenFlow Controller if there was no echo reply or message from the controller. (1-60)

- **tcp-buffer-size num**
  Configures the TCP buffer size for socket connection to OpenFlow controllers configured for the logical-switch in the pfc-channel mode (2–32).

- **dpid string**
  Configures a unique 8-byte Datapath Identifier (DPID) for a logical switch in pfc-channel mode. Value must be entered in hex format only (starting with 0x) and must be less than 8-bytes.

- **admin-state enable**
  Enables the Logical Switch.

- **admin-state disable**
  Disables the Logical Switch.

- **normal**
  Configures the Logical Switch to run in Normal Mode.

- **api**
  Configures the Logical Switch to run in Hybrid (API) Mode. Only one (1) Logical Switch can be configured in Hybrid Mode.

- **pfc-channel**
  Configures the Logical Switch for NEC pfc-channel mode.

- **1.0**
  Configures the Logical Switch to run OpenFlow Version 1.0.

- **1.3.1**
  Configures the Logical Switch to run OpenFlow Version 1.3.1.

- **learned-mac-update enable**
  Enables the forwarding of new source learned MAC addresses to a WLAN controller.

- **learned-mac-update disable**
  Disables the forwarding of new source learned MAC address to a WLAN controller.

- **vlan_id**
  The Default VLAN for all ports assigned to the Logical Switch. Traffic on this VLAN on these ports will not carry an 802.1q tag. Traffic on all other VLANs on these ports will carry an 802.1q tag. The valid range is 2 - 4093.

- **drop | controller**
  Configures whether packets are dropped or sent to the Controller when an OpenFlow Table Miss occurs.
OpenFlow Commands

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>probe-time num</td>
<td>5 seconds</td>
</tr>
<tr>
<td>failure-detect-time num</td>
<td>4 seconds</td>
</tr>
<tr>
<td>tcp-buffer-size num</td>
<td>2 KB</td>
</tr>
<tr>
<td>dpid string</td>
<td>Top 16-bit unique index of logical switch and bottom 48 bits of router MAC</td>
</tr>
<tr>
<td>admin-state enable</td>
<td>disable</td>
</tr>
<tr>
<td>normal</td>
<td>api</td>
</tr>
<tr>
<td>normal</td>
<td>normal</td>
</tr>
<tr>
<td>1.0</td>
<td>1.3.1</td>
</tr>
<tr>
<td>1.0, 1.3.1</td>
<td></td>
</tr>
<tr>
<td>learned-mac-update enable</td>
<td>disable</td>
</tr>
<tr>
<td>drop</td>
<td>controller</td>
</tr>
<tr>
<td>drop</td>
<td></td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Up to three (3) OpenFlow Logical Switches can be configured on an OmniSwitch.
- Use the `no` form of the command to delete an OpenFlow Logical Switch and all Controller/port configurations for that Logical Switch.
- When a Logical Switch is disabled, all Controllers for that Logical Switch are operationally disabled, and flows added by those Controllers are removed.
- In Normal Mode, the switch operates as per the OpenFlow standards. In Hybrid mode, OpenFlow operates as an interface through which the Controller may add over-ride policies to the switch much like QoS. In Hybrid mode, no traffic is forwarded to the Controller(s) and AOS operates normally.
- OpenFlow versions 1.0 and 1.3.1 are both enabled by default. At least one version must be enabled.
- “vlan” is not valid if the configured mode for the Logical Switch is API. An API Logical Switch implicitly operates on all ports, link aggregates, and VLANs not assigned to other OpenFlow Logical Switches.
- OpenFlow version 1.0 and 1.3.1 use TCP port 6633.
- Enabling learned MAC update only applies if the configured mode for the Logical Switch is API.
Examples

-> openflow logical-switch vswitch1
-> openflow logical-switch vswitch1 admin-state enable
-> openflow logical-switch vswitch1 mode normal version 1.0 vlan 5
-> openflow logical-switch vswitchnc mode pfc-channel
-> no openflow logical-switch vswitch1

Release History

Release 7.3.4; command introduced

Related Commands

show openflow logical-switch Displays information about all of the configured OpenFlow Logical Switches.

MIB Objects

alaOpenflowLogicalSwitchTable
  alaOpenflowLogicalSwitch
  alaOpenflowLogicalSwitchAdminState
  alaOpenflowLogicalSwitchMode
  alaOpenflowLogicalSwitchVersions
  alaOpenflowLogicalSwitchVlan
  alaOpenflowLogicalSwitchLearnedMacUpdate
  alaOpenflowLogicalSwitchProbeTime
  alaOpenflowLogicalSwitchFailureDetectTime
  alaOpenflowLogicalSwitchDPID
  alaOpenflowLogicalSwitchTableMissAction
  alaOpenflowLogicalSwitchTCPBufferSizeTx
  alaOpenflowLogicalSwitchTCPBufferSizeRx
openflow logical-switch controller

Configures a Controller for an OpenFlow Logical Switch. You can configure up to three (3) Controllers per Logical Switch.

**openflow logical-switch name controller** `{ip_address | domain_name} [:port] [priority num] admin-state {enable | disable}`

**no openflow logical-switch name controller** `{ip_address | domain_name} [:port]`

---

**Syntax Definitions**

- **name**: The Logical Switch name (up to 32 characters).
- **ip_address**: The IP address of Controller.
- **domain_name**: The Fully Qualified Domain Name (FQDN) of the Controller. Specify a domain name up to 255 characters in length.
- **port**: The Controller IP Port (1 - 65535).
- **priority num**: Configures the priority value for the specified Controller in pfc-channel mode (0-2). 0 = highest, 2 = lowest.
- **enable**: Enables the connection to the Controller.
- **disable**: Disables the connection to the Controller.

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>6633</td>
</tr>
<tr>
<td>priority num</td>
<td>2</td>
</tr>
<tr>
<td>enable</td>
<td>disable</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to remove a Controller for a Logical Switch.
- Specify either the IPv4 address or the FQDN for the Controller. When an FQDN is specified, the switch will resolve the IP address for that domain.
• If a Logical Switch cannot connect to any of its Controllers, it runs in “Fail Secure Mode”. All flow aging, etc., continues unaffected while the Controllers are disconnected.

• Use the priority parameter to configure the priority for the specified Controller. If Controllers have the same priority, the one configured first will have priority.

Examples

-> openflow logical-switch vswitch1 controller 1.2.3.4
-> openflow logical-switch vswitch1 controller 1.2.3.4:6634
-> openflow logical-switch vswitch1 controller 1.2.3.4:6634 admin-state disable
-> openflow logical-switch vswitch1 controller 1.2.3.4:6634 priority 1
-> openflow logical-switch vswitchnec controller opendaylight.abc.com
-> openflow logical-switch vswitchnec controller opendaylight.abc.com:6635
-> openflow logical-switch vswitchnec controller opendaylight.abc.com:6635 disable
-> openflow logical-switch vswitchnec controller opendaylight.abc.com priority 1
-> no openflow logical-switch vswitch1 controller 1.2.3.4
-> no openflow logical-switch vswitchnec controller opendaylight.abc.com

Release History

Release 7.3.4; command introduced.
Release 8.5R1; domain_name parameter option added.

Related Commands

show openflow logical-switch Displays information about all of the configured OpenFlow Logical Switches.

MIB Objects

alaOpenflowControllerTable
    alaOpenflowControllerLogicalSwitch
    alaOpenflowControllerIpType
    alaOpenflowControllerIp
    alaOpenflowControllerPort
    alaOpenflowControllerAdminState
    alaOpenflowControllerPriority
openflow logical-switch interfaces

Configures a range of interfaces to/from a Logical Switch.

```
openflow logical-switch name interfaces {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2] | [type {trunk | access}] | [native-vlan vlan] | [vlan-tag vlan[-vlan2]]}
```

```
no openflow logical-switch name interfaces {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]}
```

**Syntax Definitions**

- **name**: The Logical Switch name (up to 32 characters).
- **chassis/slot/port[-port2]**: The chassis ID, slot, and port number.
- **agg_id[-agg_id2]**: The link aggregate ID number.
- **trunk**: Configures the interface type as trunk.
- **access**: Configures the interface type as access.
- **native-vlan vlan**: The default VLAN for an interface in the logical switch. Traffic on this port will be untagged for the native VLAN. Traffic on all other VLANs on this port will be tagged. (2-4093)
- **vlan-tag vlan[-vlan2]**: The list of allowed tagged VLANs for an interface. Traffic on these allowed VLAN(s) of the ports and Untagged traffic will not carry an 802.1q tag. Traffic on all other VLANs on the port will be dropped. (2-4093)

**Defaults**

<table>
<thead>
<tr>
<th>parameter</th>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>access</td>
</tr>
</tbody>
</table>

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **native-vlan** and **vlan-tag** parameters are valid only if the logical switch mode is pfc-channel.

**Examples**

- `-> openflow logical-switch vswitch1 interfaces port 1/1/1`
- `-> no openflow logical-switch vswitch1 interfaces port 1/1/1`
- `-> openflow logical-switch vswitch2 interfaces linkagg 5`
-> no openflow logical-switch vswitch2 interfaces linkagg 5
-> openflow logical-switch vswitch1 interfaces port 1/1/1-8
-> no openflow logical-switch vswitch1 interfaces port 1/1/1-8
-> openflow logical-switch vswitchnec interfaces port 1/1/20 type trunk
-> openflow logical-switch vswitchnec interfaces port 1/1/20 native-vlan 3
-> openflow logical-switch vswitchnec interfaces port 1/1/20 vlan-tag 4-5

**Release History**

Release 7.3.4; command introduced

**Related Commands**

- `show openflow logical-switch`  
  Displays information about all of the configured Logical Switches.

**MIB Objects**

- `alaOpenflowInterfaceTable`
  - `alaOpenflowInterfaceLogicalSwitch`
  - `alaOpenflowInterface`
show openflow

Displays global OpenFlow configuration parameters.

show openflow

Syntax Definitions
N/A

Defaults
N/A

Platforms Supported
This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines
N/A

Examples

`-> show openflow`
`Back-off Max : 60,`
`Idle Probe Timeout : 15`

output definitions

<table>
<thead>
<tr>
<th>Back-off Max</th>
<th>The configured maximum back off time, in seconds, for Controller connection attempts (Range = 1 - 60, Default = 60).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Probe Timeout</td>
<td>The configured idle probe timeout value, in seconds (Range = 1– 60, Default = 15).</td>
</tr>
</tbody>
</table>

Release History

Release 7.3.4; command introduced
**Related Commands**

- `openflow back-off-max`  Configures the maximum amount of time allowed for Controller connection attempts.
- `openflow idle-probe-timeout`  Configures the idle probe timeout value.

**MIB Objects**

- `alaOpenflowGlobalBackoffMax`
- `alaOpenflowGlobalIdleProbeTimeout`
show openflow logical-switch

Displays information about configured OpenFlow Logical Switches.

show openflow logical-switch [name | controllers | interfaces [vlans | port | linkagg] | details]

Syntax Definitions

name
The Logical Switch name (up to 32 characters).

controllers
The controllers assigned to this logical switch.

interfaces
The interfaces assigned to this logical switch.

details
The details of the logical switch.

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Usage Guidelines

- Enter a Logical Switch name to display only information about a specific Logical Switch.
- The DPID, TCP-Buffer-Size, Probe-Time, and Failure-Detect-Time are only applicable for a logical switch in PFC mode.

Examples

-> show openflow logical-switch

Logical Switch Admin State Mode Versions VLAN MAC Ctrlrs Intf Flows
vswitch1     Ena     Norm  1.0   1     Dis   1     4    0
vswitch2     Dis     Norm  1.0, 1.3.1 5     Dis   3     4    2
vswitchnec   Ena     PFC  1.0, 1.3.1 N/A   Dis   1     0    0

output definitions

Logical Switch The Logical Switch name
Admin State The Logical Switch administrative state (Enabled or Disabled).
Mode The Logical Switch operational Mode (Normal/API/PFC).
### versions
The OpenFlow versions enabled on the Logical Switch (1.0/1.3.1).

### VLAN
The default VLAN for all ports assigned to the Logical Switch. Zero (0) indicates no VLAN configured.

### Learn MAC
Whether new source learned MAC addresses are forwarded to a WLAN controller (Enabled or Disabled).

### Ctrlrs
The number of Controllers configured for the Logical Switch (up to three (3) Controllers can be configured per Logical Switch).

### Intf
The number of interfaces (ports and link aggregations) configured for the Logical Switch.

### flows
The number of flows pushed to the Logical Switch by its Controllers.

```
-> show openflow logical-switch controllers
<table>
<thead>
<tr>
<th>Logical Switch</th>
<th>Controller</th>
<th>Role</th>
<th>Admin State</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>vswitch1</td>
<td>192.168.2.9:6633</td>
<td>Master</td>
<td>Ena</td>
<td>Disconn</td>
</tr>
<tr>
<td>vswitch2</td>
<td>192.168.2.9:6633</td>
<td>Master</td>
<td>Ena</td>
<td>Disabled</td>
</tr>
<tr>
<td>vswitch2</td>
<td>192.168.2.10:6633</td>
<td>Equal</td>
<td>Dis</td>
<td>Disabled</td>
</tr>
<tr>
<td>vswitch2</td>
<td>192.168.2.10:6634</td>
<td>Equal</td>
<td>Ena</td>
<td>Active</td>
</tr>
<tr>
<td>vswitch2</td>
<td>192.168.2.9:6634</td>
<td>Slave</td>
<td>Ena</td>
<td>Idle</td>
</tr>
<tr>
<td>vswitchnec</td>
<td>opendaylight.abc.com:66</td>
<td>Master</td>
<td>Ena</td>
<td>Active</td>
</tr>
</tbody>
</table>
```

### Logical Switch
The Logical Switch name

### Controller
The Controller IP address or Fully Qualified Domain Name (FQDN) and port. If the FQDN is longer than 22 characters, the name may appear truncated in this field.

### Role
Current role of the Controller (Equal, Master, or Slave).

### Admin State
The Logical Switch administrative state (Enabled or Disabled).

### Oper State
Current connection state of the Controller (invalid, operDisabled, sendError, init, connecting, backoff, exchangingHello, active, idle, disconnected).

```
-> show openflow logical-switch interfaces
<table>
<thead>
<tr>
<th>Logical Switch</th>
<th>Interface</th>
<th>Mode</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>vswitch1</td>
<td>1/1/1</td>
<td>Norm</td>
<td></td>
</tr>
<tr>
<td>vswitch2</td>
<td>1/1/2</td>
<td>Norm</td>
<td></td>
</tr>
<tr>
<td>vswitch2</td>
<td>1/1/3</td>
<td>Norm</td>
<td></td>
</tr>
<tr>
<td>vswitch2</td>
<td>1/1/5</td>
<td>Norm</td>
<td></td>
</tr>
<tr>
<td>vswitch2</td>
<td>1/1/10</td>
<td>Norm</td>
<td></td>
</tr>
<tr>
<td>vswitchnec</td>
<td>1/1/5</td>
<td>PFC</td>
<td>Access</td>
</tr>
<tr>
<td>vswitchnec</td>
<td>0/5</td>
<td>PFC</td>
<td>Access</td>
</tr>
</tbody>
</table>
```

### Logical Switch
The Logical Switch name

### Interface
The interface slot/port or link aggregate ID configured for the Logical Switch.
-> show openflow logical-switch vswitchnec details
Logical-Switch: vswitchnec
DPID = 0x1234567890123456
TCP-Buffer-Size = 2 Kilobytes
Probe-Time = 5 Sec
Failure-Detect-Time = 4 Sec
Table-Miss-Action = DROP

output definitions

Mode The Logical Switch operational Mode (Normal/API/PFC).
Type The type of interface assigned to the logical switch (Access or Trunk).
• Access interfaces support only untagged ports in the native VLAN.
• Trunk interfaces support untagged ports in the native VLAN and tagged ports in other VLANs.

Release History
Release 7.3.4; command introduced

Related Commands

openflow logical-switch Configures an OpenFlow Logical Switch.
openflow logical-switch controller Configures a Controller for an OpenFlow Logical Switch. You can configure up to three (3) Controllers per Logical Switch.
openflow logical-switch interfaces Configures a range of interfaces to/from a Logical Switch.
**MIB Objects**

alaOpenflowLogicalSwitchTable
- alaOpenflowLogicalSwitch
- alaOpenflowLogicalSwitchAdminState
- alaOpenflowLogicalSwitchMode
- alaOpenflowLogicalSwitchVersions
- alaOpenflowLogicalSwitchVlan
- alaOpenflowLogicalSwitchControllerCount
- alaOpenflowLogicalSwitchInterfaceCount
- alaOpenflowLogicalSwitchFlowCount
- alaOpenflowLogicalSwitchLearnedMacUpdate
- alaOpenflowLogicalSwitchProbeTime
- alaOpenflowLogicalSwitchFailureDetectTime
- alaOpenflowLogicalSwitchDPID
- alaOpenflowLogicalSwitchTableMissAction
- alaOpenflowLogicalSwitchTCPBufferSize
68  DNS Commands

A Domain Name System resolver is an internet service that translates host names into IP addresses. Every time you use a host name, a DNS service must resolve the name to an IP address. You can configure up to three domain name servers. If the primary DNS server does not know how to translate a particular host name, it asks the secondary DNS server (if specified). If this fails, it asks the third DNS server (if specified), until the correct IP address is returned (resolved). If all DNS servers have been queried and the name is still not resolved to an IP address, the DNS resolver will fail and issue an error message.

MIB information for the DNS commands is as follows:

Filename:  ALCATEL-IND1-SYSTEM.mib
Module:    alcatelIND1SystemMIB

A summary of the available commands is listed here.

<table>
<thead>
<tr>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip domain-lookup</td>
</tr>
<tr>
<td>ip name-server</td>
</tr>
<tr>
<td>ipv6 name-server</td>
</tr>
<tr>
<td>ip domain-name</td>
</tr>
<tr>
<td>show dns</td>
</tr>
</tbody>
</table>
**ip domain-lookup**

Enables or disables the DNS resolver.

-ip domain-lookup

-no ip domain-lookup

---

**Syntax Definitions**

N/A

**Defaults**

By default, the DNS resolver is disabled.

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the **no** form of this command to disable the DNS resolver.

- You must use the **ip domain-name** command to set a default domain name for your DNS resolver(s) and the **ip name-server** command to specify up to three DNS servers to query on host lookups.

- The **ip domain-lookup** command enables the DNS resolver.

**Examples**

- `-> ip domain-lookup`
- `-> no ip domain-lookup`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip name-server</code></td>
<td>Specifies the IP addresses of up to three servers to query on a host lookup.</td>
</tr>
<tr>
<td><code>ipv6 name-server</code></td>
<td>Specifies the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.</td>
</tr>
<tr>
<td><code>ip domain-name</code></td>
<td>Sets or deletes the default domain name for DNS lookups.</td>
</tr>
<tr>
<td><code>show dns</code></td>
<td>Displays the current DNS resolver configuration and status.</td>
</tr>
</tbody>
</table>

**MIB Objects**

<table>
<thead>
<tr>
<th>Object</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>systemDNS</code></td>
</tr>
<tr>
<td><code>systemDNSEnableDnsResolver</code></td>
</tr>
</tbody>
</table>
**ip name-server**

Specify the IP addresses of up to three servers to query on a host lookup.

```
ip name-server server_address1 [server_address2 [server_address3]]
```

**Syntax Definitions**

- `server_address1`: The IP address of the primary DNS server to query for host lookup. This is the only address that is required.
- `server_address2`: The IP address of the secondary DNS server to query for host lookup. This server will be queried only if the desired host name or host IP address is not located by the primary DNS server. A second IP address is optional.
- `server_address3`: The IP address of the DNS server with the lower priority. This server will be queried only if the desired host name or IP address is not located by the primary and secondary DNS servers. A third IP address is optional.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>V72/C32</th>
<th>6900</th>
<th>X48C6/T48C6/</th>
<th>6900</th>
<th>X48C4E/V48C8/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Configuration of the DNS resolver to resolve any host query requires that you first set the default domain name with the `ip domain-name` command and enable the DNS resolver function with the `ip domain-lookup` command before you specify the IP addresses of the DNS servers by using the `ip name-server` command.

- You can configure up to three IPv4 DNS servers and three IPv6 DNS servers in a switch.

**Examples**

```
-> ip name-server 10.255.11.66
```

**Release History**

Release 7.1.1; command was introduced.
Related Commands

- **ip domain-lookup** Enables or disables the DNS resolver.
- **ip domain-name** Sets or deletes the default domain name for DNS lookups.
- **show dns** Displays the current DNS resolver configuration and status.

MIB Objects

- **systemDNS**
  - systemDNSNsAddr1
  - systemDNSNsAddr2
  - systemDNSNsAddr3
**ipv6 name-server**

Specifies the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.

```
ipv6 name-server server_ipv6_address1 [server_ipv6_address2 [server_ipv6_address3]]
```

**Syntax Definitions**

- `server_ipv6_address1`: The IPv6 address of the primary IPv6 DNS server to query for host lookup. Specifying the primary IPv6 DNS address is mandatory.
- `server_ipv6_address2`: The IPv6 address of the secondary IPv6 DNS server to query for host lookup. This server will be queried only if the desired host name is not able to be resolved by the primary IPv6 DNS server. A second IPv6 address is optional.
- `server_ipv6_address3`: The IPv6 address of the IPv6 DNS server with the lower priority. This server will be queried only if the desired host name is not able to be resolved by both the primary and secondary IPv6 DNS servers. A third IPv6 address is optional.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Configuration of the DNS resolver to resolve any host query requires that you first set the default domain name with the `ip domain-name` command and enable the DNS resolver function with the `ip domain-lookup` command before you specify the IPv6 addresses of the IPv6 DNS servers by using the `ipv6 name-server` command.
- You cannot use multicast, loopback, link-local and unspecified IPv6 addresses for specifying IPv6 DNS servers.
- You can configure up to three IPv6 DNS servers and three IPv4 DNS servers in a switch.

**Examples**

```
-> ipv6 name-server fec0::2d0:d3:f3fc
-> ipv6 name-server fe2d::2c f302::3de1:1 f1bc::202:fd40:f3
```

**Release History**
Release 7.1.1; command was introduced.

**Related Commands**

- `ip domain-lookup`: Enables or disables the DNS resolver.
- `ip domain-name`: Sets or deletes the default domain name for DNS lookups.
- `show dns`: Displays the current DNS resolver configuration and status.

**MIB Objects**

- `systemDNS`
  - `systemDNSIPv6Addr1`
  - `systemDNSIPv6Addr2`
  - `systemDNSIPv6Addr3`
**ip domain-name**

Sets or deletes the default domain name for DNS lookups.

`ip domain-name name`

`no ip domain-name`

---

**Syntax Definitions**

`name` The default domain name for host lookups.

**Defaults**

N/A

**Platforms Supported**

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th>6360</th>
<th>6465</th>
<th>6560</th>
<th>6570M</th>
<th>6860</th>
<th>6860N</th>
<th>6865</th>
<th>6900</th>
<th>6900V72/C32</th>
<th>6900X48C6/T48C6/</th>
<th>9900</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- Use the `no` form of this command to delete the default domain name.
- Use this command to set the default domain name for DNS lookups.

**Examples**

- `ip domain-name company.com`
- `no ip domain-name`

**Release History**

Release 7.1.1; command was introduced.
**Related Commands**

- **ip domain-lookup** Enables or disables the DNS resolver.
- **ip name-server** Specifies the IP addresses of up to three servers to query on a host lookup.
- **ipv6 name-server** Specifies the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.
- **show dns** Displays the current DNS resolver configuration and status.

**MIB Objects**

- systemDNS
  - systemDNSDomainName
show dns

Displays the current DNS resolver configuration and status.

show dns

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

This command is supported on the following OmniSwitch platforms:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Usage Guidelines

N/A

Examples

-> show dns
Resolver is        : enabled
domainName        : company.com
IPv4 nameServer(s): 189.202.191.14
                 : 189.202.191.15
                 : 188.255.19.1
IPv6 nameServer(s): fe2d::2c
                 : f302::3del:1
                 : f1bc::202:fd40:f3

output definitions

| Resolver is | Indicates whether the DNS resolver is enabled or disabled. |
| domainName  | Indicates the default domain name assigned to the DNS lookups. This value is set using the `ip domain-name` command. |
output definitions (continued)

| IPv4 nameServer(s) | Indicates the IP address(es) of the IPv4 DNS server(s). These addresses are set using the `ip name-server` command. |
| IPv6 nameServer(s) | Indicates the IPv6 address(es) of the IPv6 DNS server(s). These addresses are set using the `ipv6 name-server` command. |

**Release History**

Release 7.1.1; command was introduced.

**Related Commands**

- `ip domain-lookup` Enables or disables the DNS resolver.
- `ip name-server` Specifies the IP addresses of up to three servers to query on a host lookup.
- `ipv6 name-server` Specify the IPv6 addresses of up to three IPv6 DNS servers to query on a host lookup.
- `ip domain-name` Sets or deletes the default domain name for DNS lookups.

**MIB Objects**

- systemDNS
  - systemDNSEnableDnsResolver
  - systemDNSDomainName
  - systemDNSNsAddr1
  - systemDNSNsAddr2
  - systemDNSNsAddr3
  - systemDNSNsIPv6Addr1
  - systemDNSNsIPv6Addr2
  - systemDNSNsIPv6Addr3
A Software License and Copyright Statements

This appendix contains ALE USA, Inc. and third-party software vendor license and copyright statements.

ALE USA, Inc. License Agreement

ALE USA, INC. SOFTWARE LICENSE AGREEMENT

IMPORTANT. Please read the terms and conditions of this license agreement carefully before opening this package.

By opening this package, you accept and agree to the terms of this license agreement. If you are not willing to be bound by the terms of this license agreement, do not open this package. Please promptly return the product and any materials in unopened form to the place where you obtained it for a full refund.

1. License Grant. This is a license, not a sales agreement, between you (the “Licensee”) and ALE USA, Inc. ALE USA, Inc. hereby grants to Licensee, and Licensee accepts, a non-exclusive license to use program media and computer software contained therein (the “Licensed Files”) and the accompanying user documentation (collectively the “Licensed Materials”), only as authorized in this License Agreement. Licensee, subject to the terms of this License Agreement, may use one copy of the Licensed Files on the Licensee’s system. Licensee agrees not to assign, sublicense, transfer, pledge, lease, rent, or share their rights under this License Agreement. Licensee may retain the program media for backup purposes with retention of the copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the Licensed Materials or any portions thereof may be made by Licensee and Licensee shall not modify, decompile, disassemble, reverse engineer, or otherwise attempt to derive the Source Code. Licensee is also advised that ALE USA, Inc. products contain embedded software known as firmware which resides in silicon. Licensee may not copy the firmware or transfer the firmware to another medium.

2. ALE USA, Inc.’s Rights. Licensee acknowledges and agrees that the Licensed Materials are the sole property of ALE USA, Inc. and its licensors (herein “its licensors”), protected by U.S. copyright law, trademark law, and are licensed on a right to use basis. Licensee further acknowledges and agrees that all rights, title, and interest in and to the Licensed Materials are and shall remain with ALE USA, Inc. and its licensors and that no such right, license, or interest shall be asserted with respect to such copyrights and trademarks. This License Agreement does not convey to Licensee an interest in or to the Licensed Materials, but only a limited right to use revocable in accordance with the terms of this License Agreement.
3. **Confidentiality.** ALE USA, Inc. considers the Licensed Files to contain valuable trade secrets of ALE USA, Inc., the unauthorized disclosure of which could cause irreparable harm to ALE USA, Inc.. Except as expressly set forth herein, Licensee agrees to use reasonable efforts not to disclose the Licensed Files to any third party and not to use the Licensed Files other than for the purpose authorized by this License Agreement. This confidentiality obligation shall continue after any termination of this License Agreement.

4. **Indemnity.** Licensee agrees to indemnify, defend and hold ALE USA, Inc. harmless from any claim, lawsuit, legal proceeding, settlement or judgment (including without limitation ALE USA, Inc.’s reasonable United States and local attorneys’ and expert witnesses’ fees and costs) arising out of or in connection with the unauthorized copying, marketing, performance or distribution of the Licensed Files.

5. **Limited Warranty.** ALE USA, Inc. warrants, for Licensee’s benefit alone, that the program media shall, for a period of ninety (90) days from the date of commencement of this License Agreement (referred to as the Warranty Period), be free from defects in material and workmanship. ALE USA, Inc. further warrants, for Licensee benefit alone, that during the Warranty Period the Licensed Files shall operate substantially in accordance with the functional specifications in the User Guide. If during the Warranty Period, a defect in the Licensed Files appears, Licensee may return the Licensed Files to ALE USA, Inc. for either replacement or, if so elected by ALE USA, Inc., refund of amounts paid by Licensee under this License Agreement. EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE LICENSED MATERIALS ARE LICENSED “AS IS” AND ALE USA, INC. AND ITS LICENSORS DISCLAIM ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO LICENSEE. THIS WARRANTY GIVES THE LICENSEE SPECIFIC LEGAL RIGHTS. LICENSEE MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM STATE TO STATE.

6. **Limitation of Liability.** ALE USA, Inc.’s cumulative liability to Licensee or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this License Agreement shall not exceed the license fee paid to ALE USA, Inc. for the Licensed Materials. IN NO EVENT SHALL ALE USA, INC. BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR EXEMPLARY DAMAGES OR LOST PROFITS, EVEN IF ALE USA, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION TO INCIDENTAL OR CONSEQUENTIAL DAMAGES MAY NOT APPLY TO LICENSEE.

7. **Export Control.** This product is subject to the jurisdiction of the United States. Licensee may not export or reexport the Licensed Files, without complying with all United States export laws and regulations, including but not limited to (i) obtaining prior authorization from the U.S. Department of Commerce if a validated export license is required, and (ii) obtaining “written assurances” from licensees, if required.

8. **Support and Maintenance.** Except as may be provided in a separate agreement between ALE USA, Inc. and Licensee, if any, ALE USA, Inc. is under no obligation to maintain or support the copies of the Licensed Files made and distributed hereunder and ALE USA, Inc. has no obligation to furnish Licensee with any further assistance, documentation or information of any nature or kind.

9. **Term.** This License Agreement is effective upon Licensee opening this package and shall continue until terminated. Licensee may terminate this License Agreement at any time by returning the Licensed Materials and all copies thereof and extracts therefrom to ALE USA, Inc. and certifying to ALE USA, Inc. in writing that all Licensed Materials and all copies thereof and extracts therefrom have been returned or erased by the memory of Licensee’s computer or made non-readable. ALE USA, Inc. may terminate this License Agreement upon the breach by Licensee of any term hereof. Upon such termination by
ALE USA, Inc., Licensee agrees to return to ALE USA, Inc. or destroy the Licensed Materials and all copies and portions thereof.

10. **Governing Law.** This License Agreement shall be construed and governed in accordance with the laws of the State of California.

11. **Severability.** Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms herein.

12. **No Waiver.** The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

13. **Notes to United States Government Users.** Software and documentation are provided with restricted rights. Use, duplication or disclosure by the government is subject to (i) restrictions set forth in GSA ADP Schedule Contract with ALE USA, Inc.’s reseller(s), or (ii) restrictions set forth in subparagraph (c) (1) and (2) of 48 CFR 52.227-19, as applicable.

14. **Third Party Materials.** Licensee is notified that the Licensed Files contain third party software and materials licensed to ALE USA, Inc. by certain third party licensors. Some third party licensors are third part beneficiaries to this License Agreement with full rights of enforcement. Please refer to the section entitled “Third Party Licenses and Notices” on page -4 for the third party license and notice terms.
Third Party Licenses and Notices

Legal Notices applicable to any software distributed alone or in connection with the product to which this document pertains, are contained in files within the software itself located at: /\texttt{flash/foss}.

Also, if needed, we provide all FOSS (Free and Open Source Software) source code used in this release at the following URL: https://github.com/Alcatel-LucentEnterpriseData.
CLI Quick Reference

Ethernet Port Commands

**interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]}`
`{admin-state | autoneg | epp, enable | disable}`

`{slot chassis/slot | port chassis/slot/port [-port2]} speed {10 | 100 | 1000 | 2500 | 10000 | 40000 | 100000 | 2000 | 4000 | 8000 | auto | max {100 | 1000 | 4000 | 8000}}`

`{slot chassis/slot | port chassis/slot/port[-port2]} crossover {auto | mdix | mdi}`

`{slot chassis/slot | port chassis/slot/port[-port2]} duplex {full | half | auto}`

`clear interfaces {slot chassis/slot | port chassis/slot/port[-port2]} {alias | description}`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} status`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} capability`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} counters`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} counters errors`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} speed {10 | 100 | 1000 | 2500 | 10000 | 40000 | 100000 | 2000 | 4000 | 8000 | auto | max {100 | 1000 | 4000 | 8000}}`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} max-frame-size`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} duplex {full | half | auto}`

**show interfaces** `{slot chassis/slot | port chassis/slot/port[-port2]} description`
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} beacon [admin-status {enable | disable}] [led-color color] [led-mode {solid | activity}]
no interfaces {slot chassis/slot | port chassis/slot/port[-port2]} beacon
show interfaces {slot chassis/slot | port chassis/slot/port[-port2]} beacon
interfaces ptp admin-state [enable | disable] [loopback-portlist chassis/slot/port chassis/slot/port [priority [num | default]]]
interfaces port chassis/slot/port ptp p2p admin-state [enable | disable]
show interfaces ptp config
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} macesec admin-state [enable | disable] [mode [static sci-rx [hex-num] key-chain keychain_id [encryption] sci-tx [hex-num] key-chain keychain_id [encryption]]]
dynamic [keychain cak_keychain_id [server-priority priority] [radius]] [transmit-interval tx_interval] [encryption]]
no interfaces {slot chassis/slot | port chassis/slot/port[-port2]} macesec [sci-rx [hex-num] sci-tx] [keychain] [encryption]
interfaces {slot chassis/slot | port chassis/slot/port[-port2]} macesec key-rotation [max-session-time num | default]
show interfaces macesec [chassis/slot/port[-port2]]
show interfaces macesec static [chassis/slot/port[-port2]]
show interfaces macesec dynamic [details] [chassis/slot/port[-port2]]
show interfaces macesec statistics [chassis/slot/port[-port2]]
show interfaces macesec dynamic key-rotation
clear interfaces {slot chassis/slot | port chassis/slot/port [-port2] [all]} macesec-statistics

Power over Ethernet (PoE) Commands

lanpower {chassis chassis | slot chassis/slot} service [start | stop]
lanpower port chassis/slot/port admin-state {enable | disable}
lanpower {chassis chassis | slot chassis/slot | port chassis/slot/port} type string
lanpower {chassis chassis | slot chassis/slot | port chassis/slot/port} power {milliwatts | default}
lanpower {chassis chassis | slot chassis/slot} maxpower {watts | default}
lanpower {chassis chassis | slot chassis/slot | port chassis/slot/port} priority [critical | high | low]
lanpower {chassis chassis | slot chassis/slot} ni-priority [critical | high | low]
lanpower power-rule rule-name [admin-state {enable | disable}] [power {on | off}] [at {minutes mm | time hh:mm | days [all | day [day ...] | date [date ...]} | months [all | month]] [timezone [local-server | utc | originator-server]]
no lanpower power-rule rule-name [admin-state {enable | disable}] [power {on | off}] [at {minutes mm | time hh:mm | days [all | day [day ...] | date [date ...]} | months [all | month]] [timezone [local-server | utc | originator-server]]

UDLD Commands

udld [enable | disable]
udld port chassis/slot/port[-port2] {enable | disable}
uudld [port [chassis/slot/port[-port2]]] mode [normal | aggressive]
uudld [port [chassis/slot/port[-port2]]] probe-timer seconds
no uudld [port [chassis/slot/port[-port2]]] probe-timer
udld port chassis/slot/port[-port2] echo-wait-timer seconds
no uudld [port [chassis/slot/port[-port2]]] echo-wait-timer
show uudld statistics [port chassis/slot/port]
show uudld configuration
show uudld configuration port [chassis/slot/port]
show uudld statistics port chassis/slot/port
show uudld neighbor port chassis/slot/port
show uudld status port [chassis/slot/port]
**Source Learning Commands**

- `mac-learning {vlan vlan[-vlan2] | port chassis/slot/port[-port2] | linkagg agg_id} {enable | disable}`
- `mac-learning flush {dynamic | static | multicast} [mac-address mac_address]`
- `mac-learning flush domain all {dynamic | static}`
- `mac-learning flush domain vlan {vlan vlan_id} {port chassis/slot/port | linkagg agg_id} {dynamic | static | multicast} [mac-address mac_address]`
- `mac-learning flush domain spb {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[service_id] | isid instance_id} {dynamic | static | mac-address mac_address} [mac-address mac_address]`
- `mac-learning flush domain vxlan {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[service_id] | vnid vxlan_id} {dynamic | static | mac-address mac_address} [mac-address mac_address]`
- `mac-learning flush domain l2gre {serviceid service_id | sap chassis/slot/port:encap | bind-sdp sdp_id[service_id]} {dynamic | static | mac-address mac_address} [mac-address mac_address]`
- `mac-learning local serviceid service_id [mac-address mac_address]`

**VLAN Management Commands**

- `vlan vlan_id [admin-state {enable | disable}] [name description]`
- `no vlan vlan_id`
- `vlan vlan_id-vlan_id members {port chassis/slot/port[-port]} | linkagg agg_id[-agg_id]`
- `untagged`
- `no vlan vlan_id[-vlan_id] members {port chassis/slot/port[-port]} | linkagg agg_id[-agg_id]`
- `vlan vlan_id-vlan_id members {port chassis/slot/port[-port]} | linkagg agg_id[-agg_id]`
- `tagged`
- `no vlan vlan_id-vlan_id members {port chassis/slot/port[-port]} | linkagg agg_id[-agg_id]`
- `vlan vlan_id mtu-ip size`
- `show vlan [vlan_id]`
- `show vlan [vlan_id-vlan_id] members {port chassis/slot/port[-port]} | linkagg agg_id[-agg_id]`
- `pvlan vlan_id[-vlan_id] [admin-state {enable | disable}] [name description] mtu-ip size`
- `no pvlan vlan_id[-vlan_id]`
- `pvlan vlan_id secondary vlan_id[-vlan_id] type {isolated | community}`
no pvlan vlan_id secondary vlan_id[-vlan_id]
 pvlan vlan_id members [port chassis/slot/port[-port] | linkagg agg_id[-agg_id]] {tagged | untagged} [isl]
 no pvlan vlan_id members [port chassis/slot/port[-port] | linkagg agg_id[-agg_id]]
 show pvlan [vlan_id-vlan_id]
 show pvlan [vlan_id] members

High Availability VLAN Commands

server-cluster cluster_id [name cluster_name] [mode {L2 | L3}] [admin-state {enable | disable}]
 no server-cluster cluster_id
 server-cluster cluster_id vlan vlan_id
 server-cluster cluster_id mac-address mac_address
 server-cluster cluster_id ip ip_address [mac-address {static mac_address | dynamic}]
 server-cluster cluster_id igmp-mode {enable | disable}
 server-cluster cluster_id ip-multicast ipm_address
 server-cluster cluster_id port [chassis/slot/port[-port2] | all]
 no server-cluster cluster_id port [chassis/slot/port[-port2] | all]
 server-cluster cluster_id linkagg agg_id[-agg_id2]
 no server-cluster cluster_id linkagg agg_id[-agg_id2]
 show server-cluster [cluster_id [port]]

VLAN Stacking Commands

ethernet-service svlan {svlan_id[-svlan_id2]} [admin-state {enable | disable}] [name description]
 no ethernet-service svlan {svlan_id[-svlan_id2]}
 ethernet-service service-name service_name svlan vlan_id
 no ethernet-service service-name service_name service_name_vlan_id
 ethernet-service nni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] [tpid
 tpid_value] [stp | mvrp] legacy-bpdu {enable | disable}
 no ethernet-service nni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]
 ethernet-service svlan {svlan_id[-svlan_id2]} nni [port chassis/slot/port[-port2] | linkagg
 agg_id[-agg_id2]]
 no ethernet-service svlan {svlan_id[-svlan_id2]} nni [port chassis/slot/port[-port2] | linkagg
 agg_id[-agg_id2]]
 ethernet-service sap sap_id service-name service_name
 no ethernet-service sap sap_id
 ethernet-service sap sap_id uni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]
 no ethernet-service sap sap_id uni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]
 ethernet-service sap sap_id vlan {all | cvlan_id[-cvlan_id2] | untagged]
 no ethernet-service sap sap_id cvlan {all | cvlan_id[-cvlan_id2] | untagged}
 ethernet-service sap-profile sap_profile_name [bandwidth not-assigned] [shared | not-
 shared] ingress-bandwidth mbps | [cvlan-tag {preserve | translate}] priority [not-
 assigned | map-inner-to-outer-p | map-dscp-to-outer-p | fixed value] egress-bandwidth
 mbps
 no ethernet-service sap-profile sap_profile_name
 ethernet-service sap sap_id sap-profile sap_profile_name
 no ethernet-service sap sap_id
 ethernet-service uni-profile uni_profile_name [tunnel-mac address] [l2-protocol
 protocol] [peer | discard | tunnel | mac-tunnel]
 no ethernet-service uni-profile uni_profile_name
 ethernet-service uni-profile uni_profile_name inbound {tagged | untagged | both} l2-protocol
 802.1ab {peer | discard | tunnel}
 no ethernet-service uni-profile uni_profile_name
 ethernet-service uni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] uni-profile
 uni_profile_name
 ethernet-service custom-L2-protocol custom_protocol_name mac mac_address [mask mask |
 ethertype ethtype [subetype subtype] | ssap/dsap ssap/dsap pid pid]
 no ethernet-service custom-L2-protocol name
 ethernet-service custom-L2-protocol custom_protocol_name custom_protocol_name
 ethernet-service mac-tunneling {enable | disable}
 ethernet-service svlan svid1[-svid2] mac-tunneling {enable | disable}
 ethernet-service transparent-bridging [nni port chassis/slot/port[-port2] | nni linkagg
 agg_id[-agg_id2] | enable | disable]
 show ethernet-service svlan [vlan_id[-vlan_id2]]
 show ethernet-service [service-name service_name] svlan vlan_id | transparent-bridging
 show ethernet-services sap [sap_id]
 show ethernet-service port {chassis/slot/port | linkagg agg_id}
 show ethernet-service uni [port chassis/slot/port | linkagg agg_id]
 show ethernet-services uni [port chassis/slot/port | linkagg agg_id] 12pt-statistics
 clear ethernet-services uni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] 12pt-
 statistics
 show ethernet-service uni [port chassis/slot/port | linkagg agg_id]
 show ethernet-service custom-L2-profile custom_protocol_name 12pt-statistics
 clear ethernet-service uni [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] 12pt-
 statistics
 show ethernet-service custom-L2-profile [custom_protocol_name]
 show ethernet-service uni-profile [uni_profile_name] 12pt-statistics
 clear ethernet-service uni-profile [uni_profile_name] 12pt-statistics
 show ethernet-service mac-tunneling
 show ethernet-service sap-profile sap_profile_name
loopback-test profile_name destination-mac dest_address [port chassis/slot/port | linkagg agg_id] source-mac src_address vlan vlan_id [type {inward | outward {sap sap_id}}] loopback-test profile_name admin-state {enable | disable} [no] loopback-test profile_name show loopback-test [profile_name] [counters] clear loopback-test counters

Distributed Spanning Tree Commands


Shortest Path Bridging Commands

spb vlanvlan_id-bvlan_id2] [admin-state {enable | disable}] [name description] no spb vlanvlan_id spb isis vlanvlan_id ect-id ect_id spb isis control-bvlan vlan_id
show ip isis database [lsp-id lsp_id]
show spb isis nodes
show spb isis unicast-table [bvlan bvlan_id]
show spb isis services [sid instance_id] [bvlan bvlan_id]
show spb isis spf [bvlan bvlan_id [mac mac_address]]
show spb isis multicast-table [instance_id]
show spb isis multicast-sources
show spb isis multicast-sources-spf [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]

show spb isis bvlan tandem-multicast-mode {sgmode | gmode}
bvlan_id

spb isis interface [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] [admin-state {enable | disable}] [hello-interval seconds] [hello-multiplier count] [metric metric] [type {2p | multi-access}] [priority priority]

no spb isis interface [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]

spb ipvpn bind vrf [vrf_name] [default] [sid instance_id gateway ip_address [all-routes]
import-route-map route_map_name]

no spb ipvpn bind vrf [vrf_name] [default] [sid instance_id gateway ip_address]

spb ipvpn6 bind vrf [vrf_name] [default] [sid instance_id gateway ipv6_address [all-routes]
import-route-map route_map_name]

no spb ipvpn6 bind vrf [vrf_name] [default] [sid instance_id gateway ipv6_address]

instance_id [all-routes | route-map route_map_name]

no spb ipvpn6 redirect [source-vrf vrf_name] | source-isid instance_id] destination-isid
instance_id

show spb ipvpn bind [vrf [vrf_name] [default]] [sid instance_id]
show spb ipvpn redirect [vrf] [isid]
show spb ipvpn route-table [sid instance_id]

spb ipvpn6 bind vrf [vrf_name] [default] [sid instance_id gateway ipv6_address [all-routes]
import-route-map route_map_name]

no spb ipvpn6 bind vrf [vrf_name] [default] [sid instance_id gateway ipv6_address]

instance_id [all-routes | route-map route_map_name]

no spb ipvpn6 redirect [source-vrf vrf_name] | source-isid instance_id] destination-isid
instance_id

show spb ipvpn6 bind [vrf [vrf_name] [default]] [sid instance_id]
show spb ipvpn6 redirect [vrf] [isid]
show spb ipvpn6 route-table [sid instance_id]

spb isis admin-state {enable | disable}
spb isis area-address area_address
spb isis source-id [source_id] auto
spb isis control-address [all1 | all2 | allis]
spb isis spf-wait [initial-wait milliseconds] [second-wait milliseconds] max-wait milliseconds]
spb isis lsp-wait [max-wait milliseconds] [initial-waitmilliseconds] [second-wait milliseconds]
spb isis rapid-lsp-converge [sid instance_id] admin-state {enable | disable}
spb isis overload [timeout seconds]
no spb isis overload
spb isis overload-on-boot [timeout seconds]
no spb isis overload-on-boot
spb isis graceful-restart
no spb isis graceful-restart
spb isis graceful-restart helper {enable | disable}
show spb isis info
show spb isis interface [port chassis/slot/port | linkagg agg_id]
show spb isis adjacency [detail]

Service Manager Commands

service service_id[service_id2] spb isid instance_id[instance_id2] bvlan bvlan_id[:x]
no service service_id spb
service service_id pseudo-wire {enable | disable}

service service_id[service_id2] vxlan vniid {vxlans vxlans_id[vxlans_id2] | xxx.xxx.xxx[-xxx.xxx.xxx]}

no service service_id vxlan
service service_id12gre vniid {vni_id}
no service service_id12gre
service service_id description desc_info
no service service_id description

service service_id multicast-mode [head-end | tandem | hybrid]

service service_id stats {enable | disable}

service service_id vlan-xlation {enable | disable}

service service_id admin-state {enable | disable}

service service_id remove-ingress-tag {enable | disable}

service vxlan udp-port {udp_port_num} [default]

service vxlan vrf [vrf_name] [default]

service local-vrrp {enable | disable}

service l2gre reserved-vlan vlan_id[vlan_id2]
no service l2gre reserved-vlan vlan_id[vlan_id2]

service l3vpn profile
no service l3vpn profile

service l2profile l2profile_name [stp | 802.1x | 802.3ad | 802.1ab] [mvrp | gvrp | amap] [peer | drop | tunnel]
no service l2profile profile-name

service l2profile l2profile_name inbound {tagged | untagged | both} 802.1ab {peer | drop | tunnel}

no service l2profile profile-name
Loopback Detection Commands

loopback-detection {remote-origin} {enable | disable}
loopback-detection port chassis/slot/port[-port2] {remote-origin} {enable | disable}
loopback-detection-service-access {port chassis/slot/port[-port2]} linkagg agg_id[agg_id2] 
{enable | disable}
loopback-detection transmission-timer seconds
loopback-detection autorecovery-timer seconds
show loopback-detection
show loopback-detection port chassis/slot/port
show loopback-detection linkagg agg_id
show loopback-detection statistics port chassis/slot/port
show loopback-detection statistics port chassis/slot/port

Link Aggregation Commands

linkagg agg_id[agg_id2] size size [name name] [admin-state {enable | disable}]
{multi-chassis active} [hash | source-mac | destination-mac | source-and-destination-mac | source-ip | destination-ip | source-and-destination-ip | tunnel-protocol}]
no linkagg static agg_id[agg_id2]
linkagg static agg_id[agg_id2] name name
no linkagg static agg_id[agg_id2] name
linkagg static agg_id[agg_id2] wait-to-restore-time wtr_minutes
no linkagg static agg_id[agg_id2] wait-to-restore-time
linkagg static agg_id[agg_id2] loopback
linkagg static agg_id[agg_id2] loopback
linkagg static agg_id[agg_id2] admin-state {enable | disable}
linkagg static port chassis/slot/port[-port2] agg agg_id
ssh-chassis [username@chassis-id]
convert configuration to dir [reload]
show virtual-chassis [chassis-id {oper_chassis}] topology
show virtual-chassis [chassis-id oper_chassis] consistency
show virtual-chassis [chassis-id oper_chassis] vv-link vfl_id member-port [oper_chassis/]
show virtual-chassis [chassis-id oper_chassis] auto-vf-link-port [chassis/slot]
show virtual-chassis [chassis-id oper_chassis] auto-vf-link-port [slot/port]
show configuration vcm-snapshot chassis-id oper_chassis
show virtual-chassis split-protection admin-state {enable | disable}
virtual-chassis split-protection linkagg agg_id
no virtual-chassis split-protection linkagg
virtual-chassis split-protection helper admin-state {enable | disable}
virtual-chassis split-protection helper linkagg agg_id
no virtual-chassis split-protection helper linkagg
show virtual-chassis split-protection status
show virtual-chassis split-protection vc-units
show virtual-chassis split-protection helper status

### Ethernet Ring Protection Commands

erp-ring ring_id ethoam-event {chassis/slot/port | linkagg agg_id} remote-endpoint mep_id
no erp-ring ring_id ethoam-event {chassis/slot/port | linkagg agg_id}
erp-ring ring_id sap-neighbor {port chassis/slot/port | linkagg agg_id}
no erp-ring ring_id sap-neighbor {port chassis/slot/port | linkagg agg_id}
clear erp statistics [ring ring_id | port chassis/slot/port | linkagg agg_id]
show erp [ring ring_id | [port chassis/slot/port | linkagg agg_id]]
show erp statistics [ring ring_id | port chassis/slot/port | linkagg agg_id]

### Media Redundancy Protocol Commands

mrp {domain domain_index | interconnect interconnect_id} vlan vlan_id
mrp domain domain_index [name domain_name] [uuid uuid] port1 [linkagg agg_id | chassis/slot/port | slot/port] port2 [linkagg agg_id | chassis/slot/port | slot/port] [admin-role [client | manager | auto-manager]] [manager [priority priority] [linkchange-react {enable | disable} | test-default [{interval interval | count repeat_count}]]] [rt-delay-reset] [recovery-time [500ms | 200ms | 30ms | 10ms]]

### MVRP Commands

mvrp {enable | disable}
mvrp port chassis/slot/port [–port2] {enable | disable}
mvrp linkagg agg_id[agg_id2] {enable | disable}
mvrp maximum-vlan vlan_limit
mvrp port chassis/slot/port [–port2] [linkagg agg_id[agg_id2]] registration {normal | fixed | forbidden}
mvrp port chassis/slot/port [–port2] [linkagg agg_id[agg_id2]] applicant {participant | non-participant | active}
mvrp port chassis/slot/port [–port2] [linkagg agg_id[agg_id2]] timer join timer_value
mvrp port chassis/slot/port [–port2] [linkagg agg_id[agg_id2]] timer leave timer_value
802.1AB Commands

```
no lldp {port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2} timer leaveall timer_value
no lldp {port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2} timer periodic-timer
no lldp {port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2} restrict-vlan-registration vlan vlan_list
no lldp {port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2} restrict-vlan-advertisement vlan vlan_list
no lldp {linkagg agg_id1-agg_id2 | port chassis/slot/port/{port2}} static-vlan-restrict vlan vlan_list
no lldp {linkagg agg_id1-agg_id2 | port chassis/slot/port/{port2}} static-vlan-restrict vlan vlan_list
show mvrp configuration
show mvrp port [chassis/slot/port/{port2}] [enable | disable]
show mvrp linkagg [agg_id1-agg_id2] [enable | disabled]
show mvrp [port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2] timer [join | leave | leaveall | periodic-timer]
show mvrp [port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2] statistics
show mvrp [port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2] last-pdu-origin
show mvrp [port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2] vlan_restrictions
show mvrp [port chassis/slot/port/{port2} | linkagg agg_id1-agg_id2] clear-statistics

802.1AB Commands

lldp nearest-edge mode {enable | disable}
lldp transmit interval seconds
lldp transmit hold-multiplier num
lldp reinit delay seconds
lldp notification interval seconds
lldp [non-tpmr | nearest-customer | nearest-bridge | all] [port chassis/slot/port/{port2} | slot chassis/slot | chassis] lldpdu [tx | rx | tx-and-rx | disable]
lldp [non-tpmr | nearest-customer | nearest-bridge | all] [port chassis/slot/port/{port2} | slot chassis/slot | chassis] notification {enable | disable}
lldp network-policy policy_id application {voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling} vlan {untagged | priority-tag | vlan_id} [llc-priority 802.1p_value] [dscp dscp_value]
no lldp network-policy policy_id-policy_id
lldp application-tlv
```
show lldp [port chassis/slot/port[-port2]] | slot chassis/slot| local-port power-via-mdi
show lldp [port chassis/slot/port[-port2]] | slot chassis/slot| local-port power-via-mdi
measurements
show lldp agent-destination-address
lldp {chassis/slot/port | chassis/slot | chassis} trust-agent [admin-state] {enable | disable}]
[chassis-id-subtype {chassis-component | interface-alias | port-component | mac-address
 | network-address | interface-name | locally-assigned | any}]
lldp {chassis/slot/port | chassis/slot | chassis} trust-agent violation-action {trap-and-
shutdown | trap | shutdown}
show lldp [chassis/slot | chassis/slot/port] trusted remote-agent
show lldp [chassis/slot | chassis/slot/port] trust-agent

SIP Commands

sip-snooping admin-state {enable | disable}
sip-snooping {port chassis/slot/port[-port2]} | linkagg agg_num | admin-state {enable | disable}
sip-snooping {port chassis/slot/port[-port2]| linkagg agg_num} mode {force-edge | force-
non-edge | automatic}
sip-snooping trusted-server [ip_address1 ip_address2 ip_address ...ip_address8]
no sip-snooping trusted-server {ip_address | all}
sip-snooping sip-control dscp num
sip-snooping sip-control no dscp
sip-snooping sos-call number string1 string2 ... string4
no sip-snooping sos-call number {string | all}
sip-snooping sos-call dscp num
sip-snooping udp-port udp-port1 udp-port 2 ... udp-port 8
no sip-snooping udp-port {udp-port | all}
sip-snooping tcp-port tcp-port1 tcp-port 2 ... tcp-port 8
no sip-snooping tcp-port {tcp-port | all}
sip-snooping threshold {audio | video | other} {jitter jitter_ms_num | packet-lost % num |
round-trip-delay round_trip_delay_ms_num | t-factor rfactor_num | mos mos_num}
sip-snooping logging-threshold num-of-calls num
show sip-snooping call-records {active-calls | ended-calls} [full | threshold-violation]
clear sip-snooping statistics
show sip-snooping config
show sip-snooping ports
show sip-snooping statistics
show sip-snooping registered-clients

Automatic Fabric Commands

auto-fabric admin-state {enable | disable} {remove-global-config | remove-vc-reload}
auto-fabric interface chassis/slot/port[-port2] admin-state {enable | disable}

IP Commands

ip interface [if_name | emp | master emp | local chassis-id chassis] [{address | vip-address}
ip_address] [mask subnet_mask] [admin-state {enable | disable}] [vlan vlan_id | service
service_id] [forward | no forward] [local-proxy-arp | no local-proxy-arp] [c2 | snap]
[primary | no primary]
no ip interface if_name
ip interface if_name address ip_address[mask vlan vlan_id rtr-port {port chassis/slot/port |
linkagg agg_id} {tagged | untagged}
no ip interface if_name [tunnel [source ip_address] [destination ip_address] [protocol {ipip |
gre}]
no ip interface dhcp-client [vlan vlan_id] [vsi-accept-filter filter-string | server-preference]
ip interface dhcp-client [vlan vlan_id] [vsi-accept-filter filter-string | server-preference]
release | renew] [option-60 opt60_string] [admin {enable | disable}] [local-proxy-arp | no local-proxy-arp]
no ip interface dhcp-client
ip interface dhcp-client no server-preference
ip router primary-address ip_address
ip router router-id ip_address
ip static-route ip_address [mask mask] [gateway {gateway_address | null} [tag num] [name
string] | interface interface_name | follows ip_address] [metric metric]
no ip static-route ip_address [mask mask] [gateway {gateway_address | null} | interface
interface_name | follows ip_address] [metric metric]
no ip static-route all bfd-state {enable | disable}
no ip static-route all bfd-state {enable | disable}
no ip static-route ipv4_prefix/pfx_length gateway ipv4_host_address bfd-state {enable | disable}
[vrf vrf_name] ip route-pref {spb-mgmt | static | ospf | isisl2 | isis1 | rip | ebgp | ibgp | import}
value
ip default-ttl hops
ping [ip_address | hostname] [source-interface ip_interface] [count count] [size packet_size]
[interval seconds] [timeout seconds] [data-pattern string] [downtime | frag | tos | val]
traceroute [ip_address | hostname] [max-hop max_hop_count] [min-hop min_hop_count]
[source-interface ip_interface] [probes probe_count] [timeout seconds] [port
port_number_value]
[vrf vrf_name] ip directed-broadcast {enable | disable}
[vrf vrf_name] ip directed-broadcast trusted-source-ip {ip_address/mask | ip_address mask subnet_mask} [destination-ip {ip_address/mask | ip_address destination-mask subnet_mask} | destination-vlan [vlan_id {vlan_id} -> vlan_id]]
[vrf vrf_name] no ip directed-broadcast trusted-source-ip {ip_address/mask | ip_address mask subnet_mask}
[vrf vrf_name] ip directed-broadcast clear [trusted-source-ip {ip_address/mask | ip_address mask subnet_mask}]
[vrf vrf_name] show ip directed-broadcast [trusted-source-ip {ip_address/mask | ip_address mask subnet_mask}]
[vrf vrf_name] ip service {all | service_name | port service_port} admin-state {enable | disable}
ip service {service_name} port {default | service_port}
[vrf vrf_name] ip service source-ip {Loopback0 | interface_name | [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
[vrf vrf_name] no ip service source-ip {Loopback0 | interface_name | [tftp] [telnet] [tacacs] [swlog] [ssh] [snmp] [sflow] [radius] [ntp] [ldap] [ftp] [dns] [all]
[vrf vrf_name] ip redist {local | static | rip | ospf | isis | bgp | spb-mgmt | import} into {rip | ospf | isis | bgp | spb-mgmt} {all-routes | route-map route_map_name} [admin-state {enable | disable}]
no ip redist {local | static | rip | ospf | isis | bgp | spb-mgmt | import} into {rip | ospf | isis | bgp | spb-mgmt} {all-routes | route-map route_map_name}
ip access-list access_list_name
no ip access-list access_list_name
ip access-list access_list_name address address/prefixLen [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
no ip access-list access_list_name address address/prefixLen
ip route-map route_map_name [sequence-number number] action {permit | deny}
no ip route-map route_map_name [sequence-number number]
ip route-map route_map_name [sequence-number number] match ip-address {access_list_name | ip_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}]} [permit | deny]
no ip route-map route_map_name [sequence-number number] match ip-address {access_list_name | ip_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}]} [permit | deny]
ip route-map route_map_name [sequence-number number] match IPv6-address {access_list_name | ipv6_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}]} [permit | deny]
no ip route-map route_map_name [sequence-number number] match IPv6-address {access_list_name | ipv6_address/prefixLen [redist-control {all-subnets | no-subnets | aggregate}]} [permit | deny]
ip route-map route_map_name [sequence-number number] match ip-next-hop {access_list_name | ip_address/prefixLen [permit | deny]}

no ip route-map route_map_name [sequence-number number] match ip-next-hop {access_list_name | ip_address/prefixLen [permit | deny]}
ip route-map route_map_name [sequence-number number] match ipv6-next-hop {access_list_name | ipv6_address/prefixLen [permit | deny]}
no ip route-map route_map_name [sequence-number number] match ipv6-next-hop {access_list_name | ipv6_address/prefixLen [permit | deny]}
ip route-map route_map_name [sequence-number number] match tag tag-number
no ip route-map route_map_name [sequence-number number] match tag tag_number
ip route-map route_map_name [sequence-number number] match ip4-interface interface_name
no ip route-map route_map_name [sequence-number number] match ipv4-interface interface_name
ip route-map route_map_name [sequence-number number] match ip6-interface interface_name
no ip route-map route_map_name [sequence-number number] match ipv6-interface interface_name
ip route-map route_map_name [sequence-number number] match metric metric [deviation deviation]
no ip route-map route_map_name [sequence-number number] match metric metric [deviation deviation]
ip route-map route_map_name [sequence-number number] match route-type {internal | external [type1 | type2] | level1 | level2}
no ip route-map route_map_name [sequence-number number] match route-type {internal | external [type1 | type2] | level1 | level2}
ip route-map route_map_name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp} no ip route-map route_map_name [sequence-number number] match protocol {local | static | rip | ospf | isis | bgp}
ip route-map route_map_name [sequence-number number] name name
no ip route-map route_map_name [sequence-number number] name name
ip route-map route_map_name [sequence-number number] set metric metric [effect {add | subtract | replace | none}]
no ip route-map route_map_name [sequence-number number] set metric metric [effect {add | subtract | replace | none}]
ip route-map route_map_name [sequence-number number] set metric-type {internal | external [type1 | type2]}
no ip route-map route_map_name [sequence-number number] set metric-type {internal | external [type1 | type2]}
ip route-map route_map_name [sequence-number number] set tag tag-number
no ip route-map route_map_name [sequence-number number] set tag tag_number
ip route-map route_map_name [sequence-number number] set community community_string
no ip route-map route_map_name [sequence-number number] set community community_string
ip route-map route_map_name [sequence-number number] set local-preference value
no ipv6 interface if_name
ipv6 interface if_name trt-port {port chassis/slot/port | linkagg agg_id} {tagged | untagged}
  vlan vlan_id
ipv6 interface if_name tunnel {source ipv4_source destination ipv4_destination}
ipv6 address ipv6_address/prefix_length {if_name | loopback}
no ipv6 address ipv6_address {if_name | loopback}
ipv6 address ipv6_prefix cui-64 {if_name | loopback}
no ipv6 address ipv6_prefix cui-64 {if_name | loopback}
ipv6 address global-id { [generate] [globalID]
ipv6 address local-unicast {global-id globalID} [subnet-id subnetID] [interface-id interfaceID]
  | cui-64} [prefix-length prefixLength] {if_name | loopback}
no ipv6 address local-unicast {global-id globalID} [subnet-id subnetID] [interface-id interfaceID]
  | cui-64} [prefix-length prefixLength] {if_name | loopback}
ipv6 hop-limit value
no ipv6 hop-limit
ipv6 mtu-lifetime time
ipv6 neighbor stale-lifetime stale-lifetime
ipv6 neighbor ipv6_address/ipv6_address {if_name} {port chassis/slot/port | linkagg agg_id}
no ipv6 neighbor ipv6_address {if_name}
ipv6 neighbor limit count
no ipv6 neighbor limit
ipv6 neighbor vrf-limit count
no ipv6 neighbor vrf-limit
ipv6 ra-filter if-name {admin-state {enable | disable}}
no ipv6 ra-filter if-name
ipv6 ra-filter if-name trusted {port chassis/slot/port | linkagg agg_id}
no ipv6 ra-filter if-name trusted {port chassis/slot/port | linkagg agg_id}
ipv6 prefix ipv6_address/prefix_length if_name {valid-lifetime time} [preferred-lifetime]
  [on-link-flag {true | false}] [autonomous-flag {true | false}] if_name
no ipv6 prefix ipv6_address/prefix_length if_name
ipv6 static-route ipv6_prefix/prefix_length gateway {ipv6_address | null} [tag num] [name string] if_name [emp] [metric metric]
no ipv6 static-route ipv6_prefix/prefix_length gateway {ipv6_address | null} if_name [emp]
ipv6 static-route all bfd-state {enable | disable}
ipv6 static-route ipv6_prefix/pfx_length gateway ipv6_host_address bfd-state {enable | disable}
ipv6 route-pref {static | ospf | rip | bgpp | isis1 | isis2 | import} value
ipv6 virtual-source-mac {on | off}
ipv6 echo {anycast | multicast}
no ipv6 echo {anycast | multicast}
ipv6 icmp rate-limit [interval number] [burst number]
no ipv6 icmp rate-limit

ping6 {ipv6_address | hostname | if_name} [count count] [size data_size] [interval seconds]
traceroute6 {ipv6_address | hostname} | if_name | [max-hop hop_count] [dest-port port_number] [probe-count probe] [size size] [host-names {yes | no}]
modify boot parameters
show ipv6 icmp statistics [if_name]
show ipv6 interface [if_name | loopback]
show ipv6 emp-interface
show ipv6 emp-routes
show ipv6 pmu table
show ipv6 ra-filter [if-name]
show ipv6 neighbors ipv6_prefix/prefix_length | if_name | hw hardware_address | static
clear ipv6 neighbors
show ipv6 prefixes
show ipv6 routes [ipv6_prefix/prefix_length | summary | protocol [bgp import | isis | local | ospf | rip | static]]
show ipv6 route-prefix
show ipv6 route database [protocol type | gateway ipv6_address | dest ipv6_prefix/ prefix_length]
show ipv6 tcp connections
show ipv6 tcp listeners
show ipv6 traffic [if_name]
show ipv6 tunnel configured
show ipv6 tunnel 6to4
show ipv6 udp ports
show ipv6 information
ipv6 redis {local | static | rip | ospf | isis | bgp | import} into {rip | ospf | isis | bgp} {all-routes | route-map route_map_name} [admin-state {enable | disable}]
ipv6 access-list access_list_name
no ipv6 access-list access_list_name
ipv6 access-list access_list_name address address/prefixLen [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
o ipv6 access-list access_list_name address address/prefixLen
show ipv6 access-list access_list_name address address/prefixLen
ipv6 access-list access_list_name address address/prefixLen [action {permit | deny}] [redist-control {all-subnets | no-subnets | aggregate}]
o ipv6 access-list access_list_name address address/prefixLen
ipv6 prefix ipv6_address/prefix_length if_name {valid-lifetime time} [valid-lifetime]
no ipv6 prefix ipv6_address/prefix_length if_name
ipv6 virtual-source-mac {on | off}
ipv6 echo {anycast | multicast}
no ipv6 echo {anycast | multicast}
ipv6 icmp rate-limit [interval number] [burst number]
no ipv6 icmp rate-limit

OmniSwitch AOS Release 8 CLI Reference Guide April 2023
**IPsec Commands**

- `ipsec key name {sa-authentication | sa-encryption} [encrypted] key`
- `no ipsec key name {sa-authentication | sa-encryption}`
- `ipsec security-key [old_key] new_key`
- `ipsec policy name [service {telnet | ftp | ssh | snmp | http | https}] [priority priority] [source {ipv6_address|ipv4_address}[prefix_length]] [port port] [destination {ipv6_address|ipv4_address}[prefix_length]] [port port] [protocol {any | icmp6 [type type] | tcp | udp | ospf | vrrp | number protocol}] [in | out] [discard | ipsec | none] [description description] [admin-state {enable | disable}]`
- `no ipsec policy name`
- `ipsec policy name rule index [ah | esp]`
- `no ipsec policy name`
- `ipsec sa name {esp | ah} [source {ipv6_address | ipv4_address}] [destination {ipv6_address | ipv4_address}] [spi spi] [encryption {null | 3des-cbc | aes-cbc [key-size key_length]}] [authentication {none | hmac-md5 | hmac-sha1 | hmac-sha256 | hmac-sha384 | hmac-sha512 | aes-xcbc-mac}] [description description] [admin-state {enable | disable}]`
- `no ipsec sa name`
- `ipsec default-discard {ipv4 | ipv6} admin-state {enable | disable}`
- `show ipsec policy [name | ipv4 | ipv6]`
- `show ipsec sa [name] [esp | ah] [source ipv6_address | ipv4_address] [destination ipv6_address | ipv4_address] [spi] [encryption null | 3des-cbc | aes-cbc [key-size key_length]] [authentication none | hmac-md5 | hmac-sha1 | hmac-sha256 | hmac-sha384 | hmac-sha512 | aes-xcbc-mac] [description description] [admin-state enable | disable]`
- `show ipsec statistics`

**RIP Commands**

- `ip load rip`
- `ip rip admin-state {enable | disable}`
- `ip rip interface {interface_name}`
- `no ip rip interface {interface_name}`
- `ip rip interface {interface_name} admin-state {enable | disable}`
- `ip rip interface {interface_name} metric value`
- `ip rip interface {interface_name} send-version {none | v1 | v1compatible | v2}`
- `ip rip interface {interface_name} receive-version {v1 | v2 | both | none}`
- `ip rip interface {interface_name} ingress-filter {filter_name}`
- `ip rip interface {interface_name} egress-filter {filter_name}`
- `ip rip force-hold-down-timer seconds`
- `ip rip host-route`
- `no ip rip host-route`
- `ip rip route-tag value`
- `ip rip interface {interface_name} auth-type {none | simple | md5}`
- `ip rip interface {interface_name} key-key string`
- `ip rip update-interval seconds`
- `ip rip invalid-timer seconds`
- `ip rip garbage-timer seconds`
- `ip rip hold-down-timer seconds`
- `show ip rip`
- `show ip rip routes [ip_address ip_mask]`
- `show ip rip interface [interface_name]`
- `show ip rip peer [ip_address]`
- `ipv6 load rip`
- `ipv6 rip admin-state {enable | disable}`
- `ipv6 rip invalid-timer seconds`
- `ipv6 rip garbage-timer seconds`
- `ipv6 rip hold-down-timer seconds`
- `ipv6 rip jitter value`
- `ipv6 rip route-tag value`
- `ipv6 rip update-interval seconds`
- `ipv6 rip triggered-sends {all | updated-only | none}`
- `ipv6 rip interface if_name`
- `no ipv6 rip interface if_name`
- `ipv6 rip interface if_name metric value`
- `ipv6 rip interface if_name recv-status {enable | disable}`
- `ipv6 rip interface if_name send-status {enable | disable}`
- `ipv6 rip interface if_name horizon {none | split-only | poison}`
- `show ipv6 rip`
- `show ipv6 rip interface [if_name]`
- `show ipv6 rip peer [ipv6_address]`
- `show ipv6 rip routes [dest ipv6_prefix/prefix_length | gateway ipv6_addr | detail ipv6_prefix/prefix_length]`

**BFD Commands**

- `ip bfd admin-state {enable | disable}`
- `ip bfd transmit transmit_interval`
- `ip bfd receive receive_interval`
- `ip bfd multiplier num`
- `ip bfd echo-interval echo_interval`
- `{ip | ipv6} bfd interface if_name`
- `no {ip | ipv6} bfd interface if_name`
- `{ip | ipv6} bfd interface if_name admin-state {enable | disable}`
- `{ip | ipv6} bfd interface if_name transmit transmit_interval`
- `{ip | ipv6} bfd interface if_name receive receive_interval`
- `{ip | ipv6} bfd interface if_name multiplier num`
- `{ip | ipv6} bfd interface if_name echo-interval echo_interval`
- `show ip bfd`
- `show {ip | ipv6} bfd interfaces [if_name]`
- `show {ip | ipv6} bfd sessions [session_num] [slot chassis/slot]`
DHCP Relay Commands

**ip dhcp relay admin-state** {enable | disable}
**no ip dhcp relay admin-state**

**ip dhcp relay destination ip_address**
**no ip dhcp relay destination ip_address**

**ip dhcp relay per-interface-mode**
**no ip dhcp relay per-interface-mode**

**ip dhcp relay interface if_name destination ip_address**
**no ip dhcp relay interface if_name destination ip_address**

**ip dhcp relay interface if_name admin-state** {enable | disable}
**no ip dhcp relay interface if_name admin-state**

**ip dhcp relay forward-delay seconds**
**no ip dhcp relay forward-delay**

**ip dhcp relay maximum-hops hops**
**no ip dhcp relay maximum-hops**

**ip dhcp relay insert-agent-information**
**no ip dhcp relay insert-agent-information**

**ip dhcp relay insert-agent-information format** {base-mac | system-name | user-string string}

**ip dhcp relay pxe-support**
**no ip dhcp relay pxe-support**

**show ip dhcp relay interface**
**show ip dhcp relay interface**

**ip dhcp relay clear statistics** [global-only | destination ip_address | interface if_name]
**no ip dhcp relay clear statistics**

**ip dhcp relay clear insert-agent-information error-count** [interface if_name | port chassis/slot/ port]
**no ip dhcp relay clear insert-agent-information error-count**

**show ip dhcp relay counters**

**ip helper address ip_address**
**no ip helper address ip_address**

**ip helper vlan vlan_id-vlan_id2 address ip_address**
**no ip helper vlan vlan_id-vlan_id2 address ip_address**

**ip helper standard**

**ip helper per-vlan-only**
**no ip helper per-vlan-only**

**show ip helper**
**no ip helper**

**show ip helper statistics** [global-only | server-only | address ip_address | vlan vlan_id {ip_address}]
**no ip helper statistics**

**ip udp relay port port_num** [description description]
**no ip udp relay port port_num**

**ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} [description description] [address ip_address]
**no ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} port port_num**

**show ip dhcp relay statistics**
**no show ip dhcp relay statistics**

**ip dhcp relay clear insert-agent-information error-count** [interface if_name | port chassis/slot/ port]
**no ip dhcp relay clear insert-agent-information error-count**

**show ip dhcp relay counters**

**ip helper address ip_address**
**no ip helper address ip_address**

**ip helper vlan vlan_id-vlan_id2 address ip_address**
**no ip helper vlan vlan_id-vlan_id2 address ip_address**

**ip helper standard**

**ip helper per-vlan-only**
**no ip helper per-vlan-only**

**show ip helper**
**no ip helper**

**show ip helper statistics** [global-only | server-only | address ip_address | vlan vlan_id {ip_address}]
**no ip helper statistics**

**ip udp relay port port_num** [description description]
**no ip udp relay port port_num**

**ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} [description description] [address ip_address]
**no ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} port port_num**

**show ip dhcp relay statistics**
**no show ip dhcp relay statistics**

**ip dhcp relay clear insert-agent-information error-count** [interface if_name | port chassis/slot/ port]
**no ip dhcp relay clear insert-agent-information error-count**

**show ip dhcp relay counters**

**ip helper address ip_address**
**no ip helper address ip_address**

**ip helper vlan vlan_id-vlan_id2 address ip_address**
**no ip helper vlan vlan_id-vlan_id2 address ip_address**

**ip helper standard**

**ip helper per-vlan-only**
**no ip helper per-vlan-only**

**show ip helper**
**no ip helper**

**show ip helper statistics** [global-only | server-only | address ip_address | vlan vlan_id {ip_address}]
**no ip helper statistics**

**ip udp relay port port_num** [description description]
**no ip udp relay port port_num**

**ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} [description description] [address ip_address]
**no ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} port port_num**

**show ip dhcp relay statistics**
**no show ip dhcp relay statistics**

**ip dhcp relay clear insert-agent-information error-count** [interface if_name | port chassis/slot/ port]
**no ip dhcp relay clear insert-agent-information error-count**

**show ip dhcp relay counters**

**ip helper address ip_address**
**no ip helper address ip_address**

**ip helper vlan vlan_id-vlan_id2 address ip_address**
**no ip helper vlan vlan_id-vlan_id2 address ip_address**

**ip helper standard**

**ip helper per-vlan-only**
**no ip helper per-vlan-only**

**show ip helper**
**no ip helper**

**show ip helper statistics** [global-only | server-only | address ip_address | vlan vlan_id {ip_address}]
**no ip helper statistics**

**ip udp relay port port_num** [description description]
**no ip udp relay port port_num**

**ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} [description description] [address ip_address]
**no ip udp relay service {tftp | tacacs | ntp | nbns | nbdd | dns} port port_num**

**show ip dhcp relay statistics**
**no show ip dhcp relay statistics**

**ip dhcp relay clear insert-agent-information error-count** [interface if_name | port chassis/slot/ port]
**no ip dhcp relay clear insert-agent-information error-count**

**show ip dhcp relay counters**

**ip helper address ip_address**
**no ip helper address ip_address**

**ip helper vlan vlan_id-vlan_id2 address ip_address**
**no ip helper vlan vlan_id-vlan_id2 address ip_address**

**ip helper standard**

**ip helper per-vlan-only**
**no ip helper per-vlan-only**

**show ip helper**
**no ip helper**

**show ip helper statistics** [global-only | server-only | address ip_address | vlan vlan_id {ip_address}]
**no ip helper statistics**

**ip dhcp relay dhcp-server {enable | disable}**
**no ip dhcp relay dhcp-server**

**ip dhcp relay dhcp-server restart**
**show dhcp-server leases** [ip-address ip_address | mac-address mac_address] [type {static | dynamic}]
**no show dhcp-server leases**

**ip dhcp relay dhcp-server statistics** [packets | hosts | subnets | all]
**no show dhcp-server statistics**
clear dhcp-server statistics
dhcpv6-server {enable | disable}
dhcpv6-server restart
show dhcpv6-server leases [ip- address ipv6_address] [type {static | dynamic}] [count]
show dhcpv6-server statistics [packets] [hosts] [subnets] [all]
clear dhcpv6-server statistics
dhcp-message-service {enable | disable}
dhcp-message-service restart
show message-service status
active-lease-service {enable | disable}
active-lease-service restart
show active-lease-service status
dhcp-snooping admin-state {enable | disable}
no dhcp-snooping
dhcp-snooping mac-address-verification admin-state {enable | disable}
dhcp-snooping option-82-data-insertion admin-state {enable | disable}
dhcp-snooping bypass option-82-check admin-state {enable | disable}
dhcp-snooping option-82 format [base-mac | system-name | user-string string | interface-alias
 | auto-interface-alias | ascii [{remote-id} circuit-id] | base-mac | cvlan | interface
 | interface-alias | system-name | user-string string | vlan] [delimiter string]]
no dhcp-snooping option-82 format ascii [{remote-id} circuit-id]
dhcp-snooping option-82 policy [replace | keep | drop]
dhcp-snooping vlan vlan_id[-vlan_id] [mac-address-verification | option-82-data-insertion]
 | admin-state {enable | disable}
no dhcp-snooping vlan vlan_id[-vlan_id]
dhcp-snooping port chassis/slot/port[[-port2] {block | client-only | trust}
dhcp-snooping linkagg agg_id[-agg_id2] {block | client-only | trust}
dhcp-snooping ip-source-filtering admin-state {enable | disable}
dhcp-snooping ip-source-filter [vlan vlan_id[-vlan_id2]] | port chassis/slot/port[-port2]
 | linkagg agg_id[-agg_id2]] admin-state {enable | disable}
dhcp-snooping binding admin-state {enable | disable}
dhcp-snooping binding timeout seconds
dhcp-snooping binding action {purge | renew | save}
dhcp-snooping binding persistency {enable | disable}
dhcp-snooping ipv6-source-filter [vlan vlan_id[-vlan_id2] | port chassis/slot/port[-port2]
 | linkagg agg_id[-agg_id2]] admin-state {enable | disable}
ipv6 dhcp guard vlan vlan_id[-vlan_id] [client {enable | disable}] [admin-state {enable | disable}]
no ipv6 dhcp guard vlan vlan_id[-vlan_id]
ipv6 dhcp guard vlan vlan_id trusted [port chassis/slot/port [-port2]] | linkagg agg_id[-agg_id2]]
no ipv6 dhcp guard vlan vlan_id trusted [port chassis/slot/port [-port2]] | linkagg agg_id[-agg_id2]]
show dhcpv6-snooping
show dhcpv6-snooping interfaces
show dhcpv6-snooping binding [global-address ipv6_address] [port chassis/slot/port | linkagg
agg_id]
show dhcpv6-snooping ipv6-source-filter
show ipv6 dhcp guard [vlan vlan_id]

VRRP Commands

{ip | ipv6} vrrp vrid interface if_name admin-state [enable | disable] [priority priority]
 | [preempt | no preempt] [accept | no accept] [interval centiseconds] [version {v2 | v3}]
no {ip | ipv6} vrrp vrid interface if_name
{ip | ipv6} vrrp vrid interface if_name ipv4_address | ipv6_address
{ip | ipv6} vrrp vrid interface if_name ipv4_address | ipv6_address
ip vrrp track track_id [admin-state {enable | disable}] [priority priority] [ipv4-interface if_name
 | ipv6-interface if_name] | port chassis/slot/port] | address ip_address [bfd-state {enable | disable}]
 | [delay seconds]]
no ip vrrp track track_id
ip vrrp bfd-state {enable | disable}
{ip | ipv6} vrrp vrid interface if_name track-association track_id
{ip | ipv6} vrrp vrid interface if_name no track-association track_id
ip vrrp delay seconds
ip vrrp version [v2 | v3]
  [ip | ipv6] vrrp interval centiseconds
  [ip | ipv6] vrrp priority priority
  [ip | ipv6] vrrp set [interval | priority | preempt | version | all | none] [override]
  [ip | ipv6] vrrp group vrid [interval centiseconds] [priority priority] [preempt | no preempt] [override]
  [ip | ipv6] vrrp admin-state [disable | enable | enable-all]
  [ip | ipv6] vrrp set [interval | priority | preempt | accept | version | all | none] [override]
  [ip | ipv6] vrrp group vrid admin-state [disable | enable | enable-all]
  [ip | ipv6] vrrp group vrid set [interval | priority | preempt | accept | version | all] [override]
  [ip | ipv6] vrrp vrid interface if_name group-association vrid
  [ip | ipv6] vrrp vrid interface if_name no group-association vrid
no [ip | ipv6] vrrp group vrid
  [ip | ipv6] vrrp group vrid admin-state [disable | enable | enable-all]
  [ip | ipv6] vrrp group vrid set [interval | priority | preempt | accept | version | all] [override]
  [ip | ipv6] vrrp vrid interface if_name group-association vrid
show [ip | ipv6] vrrp [vrid] statistics
show ip vrrp track [track_id]
show [ip | ipv6] [vrid] track-association [track_id]
show [ip | ipv6] vrrp group [vrid]
show [ip | ipv6] vrrp group-association [vrid]

**OSPF Commands**

- ip ospf redist-bgp-internal
- no ip ospf redist-bgp-internal
- ip ospf area area_id [summary {enable | disable}] [type {normal | stub | nssa}]
- no ip ospf area area_id
- ip ospf area area_id default-metric [cost cost] [type {ospf | type 1 | type 2}]
- no ip ospf area area_id default-metric tos
- ip ospf area area_id range [summary | nssa] ip_address subnet_mask [effect {admatching | noMatching}]
- no ip ospf area area_id range [summary | nssa] ip_address subnet_mask
- ip ospf interface [interface_name]
  - ip ospf admin-state {enable | disable}
  - no ip ospf interface [interface_name]
  - ip ospf interface [interface_name] admin-state {enable | disable}
  - no ip ospf interface [interface_name] admin-state {enable | disable}
  - ip ospf interface [interface_name] area area_id
  - ip ospf interface [interface_name] auth-key key_string
  - ip ospf interface [interface_name] auth-type {none | simple | md5 | key-chain key-chain-id}
  - ip ospf interface [interface_name] dead-interval seconds
  - ip ospf interface [interface_name] hello-interval seconds
  - ip ospf interface [interface_name] md5 key_id [enable | disable]
  - ip ospf interface [interface_name] md5 key_id key_string
  - ip ospf interface [interface_name] type {point-to-point | point-to-multipoint | broadcast | non-broadcast}
  - ip ospf interface [interface_name] cost cost
  - ip ospf interface [interface_name] poll-interval seconds
  - ip ospf interface [interface_name] priority priority
  - ip ospf interface [interface_name] retrans-interval seconds
  - ip ospf interface [interface_name] transit-delay seconds
  - ip ospf bfd-state {enable | disable}
  - ip ospf bfd-state all-interfaces {enable | disable}
  - ip ospf interface if_name bfd-state {enable | disable}
  - ip ospf interface if_name bfd-state drs-only
  - ip ospf interface if_name bfd-state all-neighbors {enable | disable}
  - ip ospf restart-support {planned-unplanned | planned-only}
  - no ip ospf restart-support
  - ip ospf restart-support
  - ip ospf restart-interval [seconds]
  - ip ospf restart-helper {admin-state {enable | disable}}
  - ip ospf restart-helper strict-lsa-checking admin-state {enable | disable}
  - ip ospf restart initiate
  - show ip ospf
  - show ip ospf border-routers [area_id] [router_id] [tcos] [gateway]
  - show ip ospf ext-lsdb [linkstate-id ls_id] [router-id router_id]
  - show ip ospf host [ip_address]
  - show ip ospf lsdb [area_id] [rtr | net | netsum | asbrsum] [linkstate-id ls_id] [router-id router_id]

OmniSwitch AOS Release 8 CLI Reference Guide   April 2023   page 18
show ip ospf neighbor [ip_address]
show ip ospf routes [ip_address mask tos gateway]
show ip ospf virtual-link [router_id]
show ip ospf virtual-neighbor area_id router_id
show ip ospf area [area_id]
show ip ospf area area_id range [summary | nssa] ip_address ip_mask
show ip ospf area area_id stub
show ip ospf interface [interface_name]
show ip ospf interface auth-info [interface_name]
show ip ospf restart

**OSPFv3 Commands**

ipv6 load ospf
ipv6 ospf admin-state {enable | disable}
ipv6 ospf host ipv6_address [area_id] [metric metric]
no ipv6 ospf host ipv6_address area_id
ipv6 ospf mtu-checking
no ipv6 ospf mtu-checking
ipv6 ospf route-tag tag
ipv6 ospf spf-timer [delay delay_seconds] [hold hold_seconds]
ipv6 ospf virtual-link area_id router router_id [dead-interval seconds] [hello-interval seconds] [retrans-interval seconds] [transit-delay seconds]
no ipv6 ospf virtual-link area_id router router_id
ipv6 ospf area area_id [type [normal | stub [default-metric metric] | nssa [default-metric metric]] | | summarize [filter]
no ipv6 ospf area area_id
ipv6 ospf area area_id [area-summary {noareasummary | sendareasummary}]
ipv6 ospf area area_id [nssa-translator-role {always | candidate}]
ipv6 ospf area area_id [nssa-translator-stab-interval interval]
ipv6 ospf area area_id nssa-summarize ipv6_address_prefix [filter]
ipv6 ospf interface interface_name
no ipv6 ospf interface interface_name
ipv6 ospf interface interface_name admin-state {enable | disable}
no ipv6 ospf interface interface_name
ipv6 ospf interface interface_name suppress-link-lsa
no ipv6 ospf interface interface_name suppress-link-lsa
ipv6 ospf interface interface_name type [broadcast | point-to-point | point-to-multipoint | nbma]
ipv6 ospf neighbor nbr_ipv6_address interface interface_name {eligible | ineligible}
no ipv6 ospf neighbor nbr_ipv6_address
ipv6 ospf interface interface_name area area_id
ipv6 ospf interface interface_name dead-interval seconds
ipv6 ospf interface interface_name hello-interval seconds

**IS-IS Commands**

ip load isis
ip isis admin-state {enable | disable}
ip isis area-id area address
no ip isis area-id area address
ip isis level-capability {level-1 | level-2 | level-1/2}
ip isis auth-check {enable | disable}
ip isis auth-type {simple {key key | encrypt-key encrypt_key} | md5 {key key | encrypt-key encrypt_key} | key-chain key_chain_id | none}
no ip isis csnp-auth
no ip is isis csnp-auth
ip isis hello-auth
no ip is isis hello-auth
ip isis pspn-auth
no ip is isis pspn-auth
ip is is lsp-lifetime seconds
no ip is is lsp-lifetime
ip isis lsp-wait {max-wait | initial-wait | second-wait} seconds
no ip isis lsp-wait {max-wait | initial-wait | second-wait}
ip isis spf-wait {max-wait seconds | initial-wait milliseconds | second-wait milliseconds}
no ip isis spf-wait {max-wait | initial-wait | second-wait}
ip isis summary-address {ip_prefix/mask | ip_prefix [netmask]} {level-1 | level-2 | level-1/2}
no ip isis summary-address {ip_prefix/mask | ip_prefix [netmask]}
ip isis overload {timeout seconds}
no ip isis overload {timeout}
ip isis overload-on-boot {timeout seconds}
no ip isis overload-on-boot {timeout seconds}
ip isis graceful-restart
no ip isis graceful-restart
ip isis graceful-restart helper {enable | disable}
ip isis strict-adjacency-check {enable | disable}
ip isis level {1 | 2} auth-type {simple {key key | encrypt-key encrypt_key} | md5 {key key | encrypt-key encrypt_key} | key-chain key_chain_id | none}
ip isis level {1 | 2} hello-auth
no ip isis level {1 | 2} hello-auth
ip isis level {1 | 2} csnp-auth
no ip isis level {1 | 2} csnp-auth
ip isis level {1 | 2} psnp-auth
no ip isis level {1 | 2} psnp-auth
ip isis level {1 | 2} wide-metrics-only
no ip isis level {1 | 2} wide-metrics-only
ip isis {activate-ipv6 | activate-ipv4}
no ip isis {activate-ipv6 | activate-ipv4}

BGP Commands

ip load bgp
ip bgp admin-state {enable | disable}
ip bgp autonomous-system value
ip bgp bestpath as-path ignore
no ip bgp bestpath as-path ignore
ip bgp cluster-id ip_address
ip bgp default local-preference value
ip bgp fast-external-failover
no ip bgp fast-external-failover
ip bgp always-compare-med
no ip bgp always-compare-med
ip bgp bestpath med missing-as-worst
no ip bgp bestpath med missing-as-worst
ip bgp client-to-client reflection
no ip bgp client-to-client reflection
ip bgp as-origin-interval seconds
no ip bgp as-origin-interval
ip bgp synchronization
no ip bgp synchronization
ip bgp confederation identifier value
ip bgp maximum-paths
no ip bgp maximum-paths
ip bgp log-neighbor-changes
no ip bgp log-neighbor-changes
ip bgp dampening [half-life half_life reuse reuse suppress suppress max-suppress-time
max_suppress_time]
no ip bgp dampening
ip bgp dampening clear
ip bgp as-number {asdot | asplain}
ip bgp aggregate-address ip_address ip_mask
no ip bgp aggregate-address ip_address ip_mask
ip bgp aggregate-address ip_address ip_mask admin-state {enable | disable}
ip bgp aggregate-address ip_address ip_mask as-set
no ip bgp aggregate-address ip_address ip_mask as-set
ip bgp aggregate-address ip_address ip_mask community {none | no-export | no-advertise | no-export-subconfed | num:num}
ip bgp aggregate-address ip_address ip_mask local-preference value
no ip bgp aggregate-address ip_address ip_mask local-preference value
ip bgp aggregate-address ip_address ip_mask metric value
no ip bgp aggregate-address ip_address ip_mask metric value
ip bgp aggregate-address ip_address ip_mask summary-only
no ip bgp aggregate-address ip_address ip_mask summary-only
ip bgp network ip_address ip_mask
no ip bgp network ip_address ip_mask
ip bgp network ip_address ip_mask admin-state {enable | disable}
ip bgp network ip_address ip_mask community {none | no-export | no-advertise | no-export-subconfed | num:num}
ip bgp network ip_address ip_mask local-preference value
no ip bgp network ip_address ip_mask local-preference value
ip bgp network ip_address ip_mask metric value
no ip bgp network ip_address ip_mask metric value
ip bgp neighbor ip_address
no ip bgp neighbor ip_address
ip bgp neighbor ip_address ttl-security num
ip bgp neighbor ip_address no ttl-security
ip bgp neighbor ip_address [activate-ipv4]
no ip bgp neighbor ip_address [activate-ipv4]
ip bgp neighbor ip_address admin-state {enable | disable}
ip bgp neighbor ip_address advertisement-interval value
ip bgp neighbor ip_address clear
ip bgp neighbor ip_address route-reflector-client
no ip bgp neighbor ip_address route-reflector-client
ip bgp neighbor ip_address default-originate
no ip bgp neighbor ip_address default-originate
ip bgp neighbor ip_address timers keepalive holdtime
ip bgp neighbor ip_address conn-retry-interval seconds
ip bgp neighbor ip_address auto-restart
ip bgp neighbor ip_address maximum-prefix maximum [warning-only]
ip bgp neighbor ip_address md5 key {string | none}
ip bgp neighbor ip_address ebgp-multihop [ttl]
no ip bgp neighbor ip_address ebgp-multihop
ip bgp neighbor ip_address description string
ip bgp neighbor ip_address next-hop-self
no ip bgp neighbor ip_address next-hop-self
ip bgp neighbor ip_address passive
no ip bgp neighbor ip_address passive
ip bgp neighbor ip_address remote-as-value
ip bgp neighbor ip_address remove-private-as
no ip bgp neighbor ip_address remove-private-as
ip bgp neighbor ip_address soft-reconfiguration
no ip bgp neighbor ip_address soft-reconfiguration
ip bgp neighbor ip_address stats-clear
ip bgp neighbor ip_address confederation neighbor ip_address
no ip bgp neighbor ip_address confederation neighbor ip_address
ip bgp neighbor ip_address update-source [interface_name]
ip bgp neighbor ip_address in-aspathlist {string | none}
ip bgp neighbor ip_address in-communitylist [string | none]
ip bgp neighbor ip_address in-prefixlist {string | none}
ip bgp neighbor ip_address in-prefix6list {string | none}
ip bgp neighbor ip_address out-aspathlist {string | none}
ip bgp neighbor ip_address out-communitylist [string | none]
ip bgp neighbor ip_address out-prefixlist {string | none}
ip bgp neighbor ip_address out-prefix6list [string | none]
ip bgp neighbor ip_address route-map {string | none} [in | out]
no ip bgp neighbor ip_address route-map {in | out}
ip bgp neighbor ip_address clear soft {in | out}
ipv6 bgp neighbor ipv6_address
ipv6 bgp neighbor ipv6_address ttl-security num
ipv6 bgp neighbor ipv6_address no ttl-security
ipv6 bgp neighbor ipv6_address [activate-ipv4]
o ipv6 bgp neighbor ipv6_address [activate-ipv4]
ipv6 bgp neighbor ipv6_address [activate-ipv6]
o ipv6 bgp neighbor ipv6_address [activate-ipv6]
ipv6 bgp neighbor ipv6_address [ipv6-next-hop ipv6_address]
ipv6 bgp neighbor ipv6_address [admin-state {enable | disable}]
ipv6 bgp neighbor ipv6_address clear
ipv6 bgp neighbor ipv6_address auto-restart
ipv6 bgp neighbor ipv6_address [remote-as value]
ipv6 bgp neighbor ipv6_address [timers num num]
ipv6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]
o ipv6 bgp neighbor ipv6_address [maximum-prefix num [warning-only]]
ipv6 bgp neighbor ipv6_address [next-hop-self]
o ipv6 bgp neighbor ipv6_address [next-hop-self]
ipv6 bgp neighbor ipv6_address [connect-retry-interval num]
ipv6 bgp neighbor ipv6_address [default-originate]
o ipv6 bgp neighbor ipv6_address [default-originate]
ipv6 bgp neighbor ipv6_address [update-source interface_name]
o ipv6 bgp neighbor ipv6_address [update-source interface_name]
ipv6 bgp neighbor ipv6_address [ipv4-next-hop ip_address]
ipv6 bgp neighbor ipv6_address advertisement-interval value
ipv6 bgp neighbor ipv6_address description string
ipv6 bgp neighbor ipv6_address ebgp-multihop [tll]
o ipv6 bgp neighbor ipv6_address ebgp-multihop
ipv6 bgp neighbor ipv6_address update-source-address ipv6_address
no ipv6 bgp neighbor ipv6_address update-source-address ipv6_address
ipv6 bgp neighbor ipv6_address passive
no ipv6 bgp neighbor ipv6_address passive
ipv6 bgp neighbor ipv6_address remove-private-as
no ipv6 bgp neighbor ipv6_address remove-private-as
ipv6 bgp neighbor ipv6_address soft-reconfiguration
no ipv6 bgp neighbor ipv6_address soft-reconfiguration
ipv6 bgp neighbor ipv6_address stats-clear
ip bgp confederation neighbor6 ipv6_address
no ip bgp confederation neighbor6 ipv6_address
ipv6 bgp neighbor ipv6_address in-aspathlist {string | none}
ipv6 bgp neighbor ipv6_address in-communitylist {string | none}
ipv6 bgp neighbor ipv6_address in-prefixlist {string | none}
ipv6 bgp neighbor ipv6_address in-prefixlist6 {string | none}
ipv6 bgp neighbor ipv6_address out-aspathlist {string | none}
ipv6 bgp neighbor ipv6_address out-communitylist {string | none}

ipv6 bgp neighbor ipv6_address out-prefixlist {string | none}
ipv6 bgp neighbor ipv6_address out-prefixlist6 {string | none}
ipv6 bgp neighbor ipv6_address route-map [string | none] [in | out]
no ipv6 bgp neighbor ipv6_address route-map [in | out]
ipv6 bgp neighbor ipv6_address clear soft [in | out]
ipv6 bgp neighbor ipv6_address route-reflector-client
no ipv6 bgp neighbor ipv6_address route-reflector-client
ipv6 bgp neighbor ipv6_address md5 key {string | none}
show ipv6 bgp neighbors [ipv6_address]
show ipv6 bgp neighbors statistics [ipv6_address]
show ipv6 bgp neighbors policy ipv6_address
show ipv6 bgp neighbors timers [ipv6_address]

Server Load Balancing Commands

ip slb admin-state {enable | disable}
ip slb reset statistics
ip slb cluster name {vip ip_address | condition string} [13 | 12]
o ip slb cluster name
ip slb cluster cluster_name admin-state {enable | disable}
ip slb cluster cluster_name ping period seconds
ip slb cluster cluster_name ping timeout milliseconds
ip slb cluster cluster_name ping retries count
ip slb cluster cluster_name probe probe_name
ip slb server ip ip_address cluster cluster_name [admin-state {enable | disable}] [weight weight]
o ip slb server ip ip_address cluster cluster_name
ip slb server ip ip_address cluster cluster_name probe probe_name
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp}
o no ip slb probe probe_name
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} timeout seconds
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} period seconds
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} port port_number
ip slb probe probe_name {ftp | http | https | imap | imaps | nntp | ping | pop | pops | smtp | tcp | udp} retries retries
ip slb probe probe_name {ftp | http} username user_name
ip slb probe probe_name {ftp | http} password password
ip slb probe probe_name {ftp | http} url url
ip slb probe probe_name {ftp | http} status status_value
ip slb probe probe_name {tcp | udp} send send_string
IP Multicast Switching Commands

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] admin-state [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] admin-state
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] flood-unknown [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] flood-unknown
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] version [version]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] version
ip multicast [port chassis/slot/port] sap port sap_id] max-group [num] [action {none | drop | replace}]
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] max-group [num]
[action {none | drop | replace}]
ip multicast static-neighbor vlan vlan_id [port chassis/slot/port | linkagg agg_id]
ip multicast static-neighbor service service_id sap [port | linkagg] [sap_id]
no ip multicast static-neighbor vlan vlan_id [port chassis/slot/port | linkagg agg_id]
no ip multicast static-neighbor service service_id sap [port | linkagg] [sap_id]
ip multicast static-neighbor vlan vlan_id [port chassis/slot/port | linkagg agg_id]
ip multicast static-group ip_address vlan vlan_id [port chassis/slot/port | linkagg agg_id]
ip multicast static-group ip_address service service_id sap [port | linkagg] [sap_id]
no ip multicast static-group ip_address vlan vlan_id [port chassis/slot/port | linkagg agg_id]
no ip multicast static-group ip_address service service_id sap [port | linkagg] [sap_id]
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] query-interval [seconds]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] query-interval [tenths_of_seconds]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] last-member-query-interval [tenths_of_seconds]
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] last-member-query-interval [tenths_of_seconds]
ip multicast [vlan vlan_id[-vlan_id2] | service service_id] query-response-interval
```

---

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] unsolicited-report-interval [seconds]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] unsolicited-report-interval
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] router-timeout [seconds]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] router-timeout
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] source-timeout [seconds]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] source-timeout
```

---

```
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querying [enable | disable] [static-source-ip ip_address]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querying [static-source-ip ip_address]
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] robustness [robustness]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] robustness
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing static-source-ip ip_address
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] spoofing static-source-ip ip_address
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zapping [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zapping
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querier-forwarding [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] querier-forwarding
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] helper-address ip_address
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] helper-address
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query [enable | disable]
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query
ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval milliseconds
no ip multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval
```

---

```
OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 24
```
ip multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] fast-join [enable | disable]
no ip multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] fast-join
ip multicast host-list host_list_name ip_address [ip_address]
no ip multicast host-list host_list_name [ip_address]
ip multicast [vlan vlan_id] ssm-map {group_address/length host_list_name | admin-state [enable | disable]}
no ip multicast [vlan vlan_id] ssm-map group_address/length
ip multicast [vlan vlan_id[:vlan_id2]] initial-packet-buffer admin-state [enable | disable]
ip multicast [vlan vlan_id[:vlan_id2]] initial-packet-buffer max-packet [num]
ip multicast [vlan vlan_id[:vlan_id2]] initial-packet-buffer max-flow [num]
ip multicast [vlan vlan_id[:vlan_id2]] initial-packet-buffer timeout [seconds]
ip multicast [vlan vlan_id[:vlan_id2]] initial-packet-buffer min-delay [milliseconds]
ip multicast display-interface-names
no ip multicast display-interface-names
ip multicast inherit-default-vrf-config
no ip multicast profile name [admin-state | flood-unknown | version | robustness | ...]
ip multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] apply-profile name
no ip multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] admin-state [enable | disable]
no ip multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] admin-state
ip multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] flood-unknown [enable | disable]
no ip multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] flood-unknown
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] version [version]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] version
ipv6 multicast [port chassis/slot/port | sap port sap_id] max-group [num] [action {none | drop | replace}]
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] max-group [num]
[no action {none | drop | replace}]
ipv6 multicast static-neighbor vlan vlan_id [port chassis/slot/port | linkagg agg_id]
ipv6 multicast static-neighbor service service_id sap [port | linkagg] {sap_id}
no ipv6 multicast static-neighbor service service_id sap [port | linkagg] {sap_id}
ipv6 multicast static-querier vlan vlan_id [port chassis/slot/port | linkagg agg_id]
ipv6 multicast static-querier service service_id sap [port | linkagg] {sap_id}
no ipv6 multicast static-querier service service_id sap [port | linkagg] {sap_id}
ipv6 multicast static-group ipv6_address vlan vlan_id [port chassis/slot/port | linkagg agg_id]
ipv6 multicast static-group ipv6_address service service_id sap [port | linkagg] {sap_id}
no ipv6 multicast static-group ipv6_address vlan vlan_id [port chassis/slot/port | linkagg agg_id]
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] query-interval [seconds]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] query-interval
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] last-member-query-interval [milliseconds]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] last-member-query-interval
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id query-response-interval [milliseconds]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id query-response-interval
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] unsolicited-report-interval [seconds]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] unsolicited-report-interval
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] router-timeout [seconds]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] router-timeout
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] source-timeout [seconds]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] source-timeout
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] querying [enable | disable] [static-source-ip ipv6_address]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] querying [static-source-ip ipv6_address]
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] robustness [robustness]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] robustness
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] spoofing [enable | disable]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id spoofing
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] spoofing static-source-ip ipv6_address
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] spoofing static-source-ip
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] zapping [enable | disable]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] zapping
ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] querier-forwarding [enable | disable]
no ipv6 multicast [vlan vlan_id[:vlan_id2]] | service service_id[:service_id2] querier-forwarding
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying [enable | disable]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] proxying
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] helper-address [ipv6_address]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] helper-address
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query [enable | disable]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] zero-based-query
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] forward-mode {asm | ssm | mac | auto}
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] forward-mode
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval milliseconds
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] update-delay-interval
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] fast-join [enable | disable]
no ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] fast-join
ipv6 multicast host-list host_list_name ipv6_address [ipv6_address]
no ipv6 multicast host-list host_list_name [ipv6_address]
ipv6 multicast [vlan vlan_id] ssm-map {group_address[/prefixLen] host_list_name | admin-state [enable | disable]}
no ipv6 multicast ssm-map group_address[/prefixLen]
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer admin-state {enable | disable}
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer max-packet [num]
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer max-flow [num]
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer timeout [seconds]
ipv6 multicast [vlan vlan_id[-vlan_id2]] initial-packet-buffer min-delay [milliseconds]
ipv6 multicast display-interface-names
no ipv6 multicast display-interface-names
ipv6 multicast inherit-default-vrf-config
no ipv6 multicast inherit-default-vrf-config
ipv6 multicast profile profile_name [admin-state | flood-unknown | version | robustness | ...]
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] apply-profile profile_name
no ipv6 multicast profile profile_name [admin-state | flood-unknown | version | robustness | ...]
ipv6 multicast [vlan vlan_id[-vlan_id2] | service service_id[-service_id2]] apply-profile
show ip multicast neighbor [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ip multicast querier [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ip multicast group [ip_address] [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ip multicast source [ip_address] [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ip multicast tunnel [ip_address] [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ip multicast host-list [host_list_name]
show ipv6 multicast ssm-map [vlan vlan_id]
show ip multicast bridge [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] | ip_address | mac_address] [all-vrf]
show ip multicast bridge-forward [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] | ip_address | mac_address] [all-vrf]
show ip multicast bidir-forward [ip_address] [all-vrf]
show ip multicast profile [profile_name]
show ipv6 multicast {port [chassis/slot/port] | sap port [sap_id]} [all-vrf]
show ipv6 multicast forward [ipv6_address] [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] | ip_address | mac_address] [all-vrf]
show ipv6 multicast neighbor [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ipv6 multicast querier [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ipv6 multicast group [ip_address] [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ipv6 multicast source [ip_address] [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ipv6 multicast tunnel [ipv6_address] [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] [all-vrf]
show ipv6 multicast bridge [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] | ipv6_address | mac_address] [all-vrf]
show ipv6 multicast bridge-forward [vlan [vlan_id[-vlan_id2] | service [service_id[-service_id2]] | ipv6_address | mac_address] [all-vrf]
show ipv6 multicast bidir-forward [ipv6_address] [all-vrf]
show ipv6 multicast profile [profile_name]

DVMRP Commands

ip load dvmrp
dvmrp admin-state {enable | disable}
PIM Commands

ip load pim
ip pim sparse admin-state {enable | disable}
ip pim bidir admin-state {enable | disable}
ip pim dense admin-state {enable | disable}
ip pim rp-hash admin-state {enable | disable}
ip pim ssm group group_address/prefix_length [[no] override] [priority priority]
no ip pim ssm group group_address/prefix_length
ip pim dense group group_address/prefix_length [[no] override] [priority priority]
no ip pim dense group group_address/prefix_length
ip pim cbsr ip_address [priority priority] [mask-length bits]
no ip pim cbsr ip_address
ip pim static-rp group_address/prefix_length rp_address [[no] bidir] [[no] override] [priority priority]
no ip pim static-rp group_address/prefix_length rp_address
ip pim anycast-rp anycast_rp_address rp_address
no ip pim anycast-rp anycast_rp_address rp_address
ip pim candidate-rp rp_address group-address/prefix_length [[no] bidir] [priority priority] [interval seconds]
no ip pim candidate-rp rp_address group-address/prefix_length
ip pim rp-threshold bps

ip pim keepalive-period seconds
ip pim max-rps number
ip pim probe-time seconds
ip pim register checksum {header | full}
ip pim register-checksum {enable | disable | force-enable}
ip pim pim-register-mtu num
ip pim register-delay num
ip pim register-suppress-timeout seconds
ip pim register-rate-limit pps
ip pim spt admin-state {enable | disable}
ip pim state-refresh-interval seconds
ip pim state-refresh-limit ticks
ip pim state-refresh ttl num
ip pim interface if_name
ip pim neighbor-loss-notification-period seconds
ip pim invalid-register-notification-period seconds
ip pim invalid-joinprune-notification-period seconds
ip pim rp-mapping-notification-period seconds
ip pim interface-election-notification-period seconds
ip pim nonbidir-hello-notification-period seconds
ip pim df-abort {enable | disable}
ip pim mbr all-sources
no ip pim mbr all-sources
ip pim df-periodic-interval seconds
ip pim bfd-state {enable | disable}
ip pim bfd-state all-interfaces {enable | disable}
ip pim interface if_name bfd-state {enable | disable}
ip pim bidir ssm-compat {enable | disable}
ip pim bidir fast-join {enable | disable}
ip pim sparse asm-fast-join {enable | disable}
ip pim sparse ssm-fast-join {enable | disable}
ip pim joinprune-packing {enable | disable}
show ip pim sparse
show ip pim dense
show ip pim ssm group
show ip pim dense group
show ip pim neighbor [ip_address]
show ip pim candidate-rp
show ip pim group-map [bsr | static-rp | ssm | dense]
show ip pim interface [if_name]
show ip pim static-rp
show ip pim anycast-rp
show ip pim cbsr
show ip pim bsr
show ip pim notifications
show ip pim grp [group_address]
show ip pim sgrp [source_address group_address]
show ip pim df-election [rp_address | if_name]
ipv6 pim sparse admin-state {enable | disable}
ipv6 pim bidir admin-state {enable | disable}
ipv6 pim dense admin-state {enable | disable}
ipv6 pim ssm group group_address/prefix_length [[no] override] [priority priority]
no ipv6 pim ssm group group_address/prefix_length
ipv6 pim dense group group_address/prefix_length [[no] override] [priority priority]
no ipv6 pim dense group group_address/prefix_length
ipv6 pim cbgr ipv6_address [priority priority] [mask-length bits]
no ipv6 pim cbgr ipv6_address
ipv6 pim static-rp group_address/prefix_length rp_address [[no] bidir] [[no] override]
[priority priority]
no ipv6 pim static-rp group_address/prefix_length rp_address
ipv6 pim candidate-rp rp_address group_address/prefix_length [[no] bidir] [priority priority]
[interval seconds]
no ipv6 pim candidate-rp rp_address group_address/prefix_length
ipv6 pim rp-switchover [enable | disable]
ipv6 pim register-rate-limit pps
ipv6 pim register-packing {enable | disable | force-enable}
ipv6 pim register-mtu num
ipv6 pim register-delay <num>
ipv6 pim spt admin-state {enable | disable}
ipv6 pim interface if_name
ipv6 pim bfd-state {enable | disable}
ipv6 pim bfd-state all-interfaces {enable | disable}
ipv6 pim interface if_name bfd-state {enable | disable}
ipv6 pim bidir ssm-compat {enable | disable}
ipv6 pim bidir fast-join {enable | disable}
ipv6 pim sparse asm-fast-join {enable | disable}
ipv6 pim sparse ssm-fast-join {enable | disable}
ipv6 pim joinprune-packing {enable | disable}
show ipv6 pim sparse
show ipv6 pim dense
show ipv6 pim ssm group
show ipv6 pim dense group
show ipv6 pim interface [if_name]
show ipv6 pim neighbor [ipv6_address] [if_name]
show ipv6 pim static-rp
show ipv6 pim anycast-rp
show ipv6 pim group-map [bsr | static-rp | ssm | dense]
show ipv6 pim candidate-rp
show ipv6 pim cbgr
show ipv6 pim bsgr
show ipv6 pim grp [group_address]
show ipv6 pim sgrp [source_address group_address]
show ipv6 pim df-election [rp_address | if_name]

Multicast Routing Commands

ip mroute-boundary if_name scoped_address mask
no ip mroute-boundary if_name scoped_address mask
ip mroute-boundary extended {enable | disable}
ip mroute interface if_name ttl threshold
ip mroute mbr admin-state {enable | disable}
ip mroute interface if_name ttl threshold
show ip mroute-boundary
show ip mroute
show ipv6 mroute
show ip mroute interface [interface_name]
show ipv6 mroute interface [interface_name]
show ip mroute-nexthop
show ipv6 mroute-nexthop
show ip mroute
show ipv6 mroute

QoS Commands

qos {enable | disable}
qos trust-ports
qos no trust-ports
qos forward log
qos no forward log
qos log console
qos no log console
qos log lines lines
qos log level level
qos no log level
qos stats interval seconds
qos phones [priority priority_value | trusted]
qos no phones
qos quarantine mac-group mac_group
qos no quarantine mac-group
qos user-port {filter | shutdown} {spoof | bgp | bpdu | rip | ospf | vrrp | dvmrp | pim | isis | dhcp-server | dns-reply}
QoS Policy Commands

policy rule rule_name [enable | disable] [precedence precedence] [condition condition]
  [action action] [validity-period name] [save] [log [log-interval seconds]] [count [packets | bytes]] [trap] [default-list]
policy rule rule_name no [validity-period | save | log | trap | default-list]
no policy rule rule_name

iec message-type message priority string
iec message-type message flush
iec show

policy validity-period name [days days] [months months] [hours hh:mm to hh:mm] [interval
  mm:dd:yy hh:mm to mm:dd:yy hh:mm]
policy validity-period name no [hours | interval]
no policy validity-period name

policy list list_name type [icmp | egress | appfip | emapcl] [enable | disable]
no policy list list_name

policy list list_name rules rule_name [rule_name2...]
policy list list_name no rules rule_name [rule_name2...]
policy network group net_group ip_address [mask net_mask] [ip_address2 [mask
  net_mask2]...]
no policy network group net_group

policy network group net_group no ip_address [mask netmask] [ip_address2 [mask
  net_mask2]...]
policy service group service_group service_name1 [service_name2...]
no policy service group service_group

policy service group service_group no service_name1 [service_name2...]
policy mac group mac_group mac_address [mask mac_mask] [mac_address2 [mask
  mac_mask2]...]
no policy mac group mac_group

policy mac group mac_group no mac_address [mask mac_mask] [mac_address2 [mask
  mac_mask2]...]

policy port group group_name {chassis//slot/port[-port2] | agg_id[-agg_id2]} [chassis//slot/
  port[-port2] | agg_id[-agg_id2]]
no policy port group group_name

policy port group group_name no {chassis//slot/port[-port2] | agg_id[-agg_id2]} [chassis//
  slot/port[-port2] | agg_id[-agg_id2]]
no policy port group group_name

policy map group map_group {value1:value2...}
no policy map group map_group

policy map group no {value1:value2...}
policy service service_name
no policy service service_name

policy service service_name protocol protocol {[source ip-port port[-port]] [destination ip-
  port port[-port]]}
no policy service service_name

policy service service_name no {source ip-port | destination ip-port}
policy service service_name source tcp-port port[-port]
no policy service service_name

policy service service_name no source tcp-port
policy service service_name destination tcp-port port[-port]
no policy service service_name

policy service service_name no destination tcp-port
policy service service_name source udp-port port[-port]
no policy service service_name

policy service service_name no source udp-port
policy service service_name destination udp-port port[-port]
no policy service service_name

policy service service_name no destination udp-port

no policy service condition condition_name

policy condition condition_name source ip {any | ip_address [mask netmask]}
policy condition condition_name no source ip

policy condition condition_name source ipv6 {any | ipv6_address [mask netmask]}
policy condition condition_name no source ipv6

policy condition condition_name destination ip ip_address [mask netmask]
policy condition condition_name no destination ip

policy condition condition_name destination ipv6 {any | ipv6_address [mask netmask]}
policy condition condition_name no destination ipv6

policy condition condition_name multicast ip ip_address [mask netmask]
policy condition condition_name no multicast ip

policy condition condition_name source network group network_group
policy condition condition_name no source network group

policy condition condition_name destination network group network_group
policy condition condition_name no destination network group

policy condition condition_name multicast network group multicast_group
policy condition condition_name no multicast network group

policy condition condition_name source tcp-port port[-port]
policy condition condition_name no source tcp-port

policy condition condition_name destination tcp-port port[-port]
no policy condition condition_name
policy condition condition_name no destination tcp-port
policy condition condition_name source udp-port port[-port]
policy condition condition_name no source udp-port
policy condition condition_name destination udp-port port[-port]
policy condition condition_name no destination udp-port
policy condition condition_name ethertype etype
policy condition condition_name no ethertype
policy condition condition_name established
policy condition condition_name no established
policy condition condition_name tcpflags [any | all] {f | s | r | p | a | u | e | w} mask {f | s | r | p | a | u | e | w}

policy condition condition_name no tcpflags
policy condition condition_name service service_name
policy condition condition_name no service
policy condition condition_name service group service_group
policy condition condition_name no service group
policy condition condition_name icmptype type
policy condition condition_name no icmptype
policy condition condition_name icmpcode code
policy condition condition_name no icmpcode
policy condition condition_name ip-protocol protocol
policy condition condition_name no ip-protocol
policy condition condition_name ipv6
policy condition condition_name no ipv6
policy condition condition_name flow-label flow_label_value
policy condition condition_name no flow-label
policy condition condition_name tos tos_value [mask tos_mask]
policy condition condition_name no tos
policy condition condition_name dscp {dscp_value[-value]} [mask dscp_mask]
policy condition condition_name no dscp
policy condition condition_name source mac mac_address [mask mac_mask]
policy condition condition_name no source mac
policy condition condition_name destination mac mac_address [mask mac_mask]
policy condition condition_name no destination mac
policy condition condition_name source mac group group_name
policy condition condition_name no source mac group
policy condition condition_name destination mac group group_name
policy condition condition_name no destination mac group
policy condition condition_name source vlan vlan_id
policy condition condition_name no source vlan
policy condition condition_name inner source-vlan vlan_id
policy condition condition_name no inner source-vlan
policy condition condition_name destination vlan vlan_id
policy condition condition_name no destination vlan

policy condition condition_name 802.1p 802.1p_value
policy condition condition_name no 802.1p
policy condition condition_name inner 802.1p 802.1p_value
policy condition condition_name no inner 802.1p
policy condition condition_name source {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
policy condition condition_name no source {port | linkagg}

policy condition condition_name destination {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
policy condition condition_name no destination {port | linkagg}

policy condition condition_name source port group group_name
policy condition condition_name no source port group
policy condition condition_name destination port group group_name
policy condition condition_name no destination port
policy condition condition_name vrf {vrf_name | default}

policy condition condition_name no vrf

policy condition condition_name fragments
policy condition condition_name no fragments
policy condition condition_name app-mon-application-group group_name
policy condition condition_name no app-mon-application-group
policy condition condition_name app-mon-application-name app_name
policy condition condition_name no app-mon-application-name
policy condition condition_name appfp-group group_name
policy condition condition_name no appfp-group

policy condition condition_name vxlan vni vxlan_id
no policy condition condition_name

policy condition condition_name vxlan inner source mac mac_address [mask mac_mask]
policy condition condition_name vxlan no source mac
policy condition condition_name vxlan inner source mac group group_name
policy condition condition_name vxlan no source mac group
policy condition condition_name vxlan inner source ip ip_address [mask netmask]
policy condition condition_name vxlan no source ip
policy condition condition_name vxlan inner source ipv6 ipv6_address [mask netmask]
policy condition condition_name vxlan no source ipv6

policy condition condition_name vxlan inner ip-protocol protocol
policy condition condition_name vxlan no ip-protocol
policy condition condition_name vxlan inner l4-port {src src_port | dest dest_port}
policy condition condition_name vxlan no l4-port
policy condition condition_name vxlan-inner udp-port
policy condition condition_name vxlan no vxlan-port

policy action action_name
policy no action action_name

policy action action_name disposition {accept | drop | deny}

policy action action_name shared
policy action action_name no shared
policy action action_name priority priority_value
policy action action_name no priority
policy action action_name maximum bandwidth bps [k | m | g | t]
policy action action_name no maximum bandwidth
policy action action_name maximum depth bytes [K (kilo) | M (mega) | G (giga) | T (tera)]
policy action action_name no maximum depth
policy action action_name cir bps [cbs bytes] [pir bps] [pbs bytes] [color-only]

show [applied] policy rule [rule_name]
show policy validity period [name]
show active policy list [list_name]
show [applied] policy list [list_name]
show policy ipv4-summary [rule_name]
show policy ipv6-summary [rule_name]

Policy Server
Commands
policy server load
policy server flush
policy server ip_address [port port_number] [admin-state {enable | disable}] [preference preference] [user user_name password password] [searchbase search_string] [ssl | no ssl]
no policy server ip_address [port port_number]
show policy server
show policy server long
show policy server statistics
show policy server rules
show policy server events

AAA Commands
aaa radius-server server_name host {hostname | ip_address | ipv6_address} [hostname2 | ip_address2 | ipv6_address2] {key secret [hash-key hash_secret] [prompt-key][salt salt | hash-salt hash_salt] [retransmit retries] [timeout seconds] [auth-port auth_port] [acct-port acct_port] [vrf-name name] [ssl | no ssl]
no aaa radius-server server_name
aaa radius-server server_name health-check [poling-interval seconds] [username user_name | password password] [hash-key hash_secret | failover]
no aaa radius-server server_name health-check [failover]
aaa radius unp-profile-precedence {tunnel-private-group-id | filter-id}
aaa test-radius-server server_name type {authentication user user_name password password [method {md5 | pap}] | accounting user user_name}
aaa tacacs+-server server_name host {hostname | ip_address | ipv6_address1} [hostname2 | ip_address2 | ipv6_address2] {key secret [prompt-key][salt salt | hash-salt hash_salt] [timeout seconds] [port port] [vrf-name name]}
no aaa tacacs+-server server
aaa tacacs command-authorization {enable | disable}
aaa ldap-server server_name host {hostname | ip_address | ipv6_address} [hostname2 | ip_address2 | ipv6_address2] dn dn_name [password super_password | prompt-password][salt salt | hash-salt hash_salt] [base search_base] [retransmit retries] [timeout seconds] [ssl | no ssl] [port port] [vrf-name name]
no aaa ldap-server server_name
system fips admin-state {enable | disable}
aaa authentication {console | telnet | ftp | http | snmp | ssh | default} server1 [server2...] [local]
no aaa authentication {console | telnet | ftp | http | snmp | ssh | default}
aaa console admin-only {enable | disable}
aaa authentication {console | telnet | ftp | http | snmp | ssh | default} default
aaa accounting session server1 [server2...] [local]
no accounting session
aaa accounting command server1 [server2...] [local]
no accounting command
aaa device-authentication {802.1x | mac | captive-portal} server1 [server2] [server3]
[server4]
no device-authentication {802.1x | mac | captive-portal}
aaa accounting {802.1x | mac | captive-portal} [server1 [server2...] | syslog ip_address [port udp_port]]
no accounting {802.1x | mac | captive-portal}
aaa accounting {802.1x | mac | captive-portal} radius calling-station-id {mac-address | ip-address}
aaa 802.1x re-authentication {enable | disable | interval seconds | trust-radius {enable | disable}}
aaa {802.1x | mac | captive-portal} interim-interval seconds [trust-radius {enable | disable}]
aaa {mac | captive-portal} session-timeout {enable | disable} [interval seconds] [trust-radius {enable | disable}]
aaa session console {enable | disable}
aaa {mac | captive-portal} inactivity-logout {enable | disable} [interval seconds]
aaa radius nas-port-id {user-string string} [default]
aaa radius nas-identifier {user-string string} [default]
aaa radius nas-ip-address {default | local-ip [ip_address]}
aaa radius mac-format {username | password | calling-station-id | called-station-id} delimiter {char | none} case {uppercase | lowercase}
aaa profile profile_name
no aaa profile profile_name
user username
no user username
password
enable super-password
user password-size min size
user password-expiration {day | disable}
user username allow-ssh {enable | disable}
user password-policy cannot-contain-username {enable | disable}
user password-policy cannot-contain-consecutive-characters {enable | disable}
user password-policy min-uppercase number
user password-policy min-uppercase number
user password-policy min-digit number
user password-policy min-nonalpha number
user password-history number
user password-min-age days
user lockout-window minutes
user lockout-threshold number
user lockout-duration minutes
user username {lockout | unlock}
show aaa server [server_name]
show aaa server server_name statistics
aaa radius-server server_name clear-statistics
show aaa authentication
show aaa device-authentication [802.1x | mac | captive-portal]
show aaa accounting [802.1x | mac | captive-portal]
show aaa [802.1x | mac | captive-portal] config
show aaa radius config
show aaa radius health-check-config
show aaa profile [profile_name]
show aaa session console config
show user [username]
show user password-policy
show user lockout-setting
show aaa priv hexa [domain or family]
show system fips
aaa switch-access mode {default | enhanced}
aaa switch-access ip-lockout-threshold number
aaa switch-access banned-ip {all | ip_address} release
aaa switch-access priv-mask {console | telnet | ssh | http | https} {read-only | read-write} {families... | domains... | all | none | all-except families...}
aaa switch-access management-stations admin-state {enable | disable}
aaa switch-access management-stations ip_address {ip_address/mask}
oo aaa switch-access management-stations ip_address
show aaa switch-access mode
show aaa switch-access ip-lockout-threshold
show aaa switch-access banned-ip
show aaa switch-access priv-mask
show aaa switch-access management-stations
show aaa switch-access hardware-self-test
show aaa switch-access process-self-test
aaa common-criteria admin-state {enable | disable}
show aaa common-criteria config
aaa certificate update-ca-certificate ca_file
aaa certificate update-crl crl_file
aaa certificate generate-rsa-key key-file key_file
aaa certificate generate-self-signed {cert_file} key {key_file} [days valid_period] {cn common_name} {on org_name} {ou org_unit} {l locality} {st state} {c country}

aaa certificate view cert_file

aaa certificate verify ca-certificate ca_cert_file certificate cert_file

aaa certificate delete cert_file

aaa certificate generate-csr {csr_file} key {key_file}

dn domain_name {cn common_name} {on org_name} {ou org_unit} {l locality} {st state} {c country}

ssl pki client validate-certificate admin-state {enable | disable}

ssl pki client mutual-authentication admin-state {enable | disable}

ssl pki server mutual-authentication admin-state {enable | disable}

ssl pki tls version {1.0 | 1.1 | 1.2}

show ssl pki config

show ssl ciphers config

show ssl ciphers all

show ssl ciphers config

show ssl ciphers admin-state {enable | disable}

show ssl ciphers all

show ssl ciphers config

show kerberos configuration

show kerberos configuration

show kerberos users {port chassis/slot/port | linkagg agg_id | mac-address mac_address | count}

show kerberos configuration

show kerberos configuration

show kerberos statistics

show kerberos statistics

show kerberos configuration

show kerberos configuration

show kerberos statistics

show kerberos statistics

Access Guardian Commands

unp dynamic-vlan-configuration

no unp dynamic-vlan-configuration

unp dynamic-profile-configuration

no unp dynamic-profile-configuration

unp delay-learning seconds

unp auth-server-down {voice} {profile1 profile_name [profile2 profile_name] [profile3 profile_name]}

no unp auth-server-down {voice} [profile1] [profile2] [profile3]

unp auth-server-down port-bounce

no unp auth-server-down port-bounce

unp auth-server-down-timeout seconds

no unp auth-server-down-timeout

unp policy validity-period policy_name [days days] [months months] [hours hh:mm to hh:mm] [interval mm:dd:yy hh:mm to mm:dd:yy hh:mm] [timezone zones]

no unp policy validity-period policy_name

days valid_period [days]{on org_name} {ou org_unit} {l locality} {st state} {c country}

unp policy validity-location policy_name [port chassis/slot/port1-port2] | linkagg agg_id-agg_id | system-name system_name | system-location system_location

no unp policy validity-location policy_name

days valid_period [days]{on org_name} {ou org_unit} {l locality} {st state} {c country}

unp redirect pause-timer seconds

no redirect pause-timer

unp redirect proxy-server-port proxy_port

no unp redirect proxy-server-port

unp redirect server {ip_address | domain_name}

no unp redirect server

unp redirect allowed-name name ip-address ip_address ip-mask ip_mask

no unp redirect allowed-name name


no unp [port chassis/slot/port1-port2] | linkagg agg_id-agg_id] force-l3-learning [port-bounce]

unp 802.1x-pass-through

no unp 802.1x-pass-through

unp ipv6-drop

no unp ipv6-drop

unp ap-mode {enable | disable} {secure {enable | disable}}

unp mac-mobility

no unp mac-mobility

unp user flush [port chassis/slot/port1-port2] | linkagg agg_id-agg_id] [sap-id linkagg]

unp 802.1x eapol-version {v1 | v3}

unp multi-untag-sap

no unp multi-untag-sap

unp profile profile_name

no unp profile profile_name

unp profile profile_name qos-policy-list list_name

no unp profile profile_name qos-policy-list

unp profile profile_name location-policy policy_name

no unp profile profile_name location-policy

unp profile profile_name period-policy policy_name

no unp profile profile_name period-policy

unp profile profile_name captive-portal-authentication

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 34
no unp classification lldp med-endpoint {ip-phone | access-point} [profile1] [profile2] [profile3]
unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [vlan-tag vlan_id | outer_vlan_id:inner_vlan_id] [profile1] [profile2] [profile3]
no unp classification authentication-type {none | mac [fail] | 802.1x [fail]} [profile1] [profile2] [profile3]
unp classification-rule rule_name [precedence precedence_value] [profile1] [profile2] [profile3]
no unp classification-rule rule_name [precedence precedence_value] [profile1] [profile2] [profile3]
captive-portal mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
captive-portal-mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
captive-portal-mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
captive-portal-mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
captive-portal-mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
captive-portal-mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
captive-portal-mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
zcaportal-mode {internal | internal dhcp [ip-lease-time seconds] [ip-renew-time seconds] [ip-rebinding-time seconds] | external}
no captive-portal mode internal
captive-portal name {ip_address | domain_name}
ocaptive-portal name
captive-portal ip-address ip_address
no captive-portal ip-address
no captive-portal success-redirect-url redirect_url
no captive-portal success-redirect-url
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal retry-count retries
no captive-portal authentication-pass [policy-list list_name | profile profile_name | profile-change {enable | disable}]
ocaptive-portal authentication-pass realm [prefix | suffix] domain domain_name
no captive-portal authentication-pass realm [prefix | suffix] domain domain_name
captive-portal-profile profile_name
captive-portal proxy-server-port proxy_port
no captive-portal proxy-server-port
captive-portal profile profile_name
captive-portal-proxy-server-port proxy_port
no captive-portal-proxy-server-port
qmr quarantine allowed-name name
no qmr quarantine allowed-name
qmr quarantine custom-proxy-port proxy_port
no qmr quarantine custom-proxy-port
show qmr
show quarantine mac group
zeroconf mdns admin-state {enable | disable}
no zeroconf mdns admin-state
zeroconf sdap admin-state {enable | disable}
no zeroconf sdap admin-state
AppMon admin-state {enable | disable}
app-mon {port chassis/slot/port[-port2]} slot chassis/slot [-slot] admin-state {enable | disable}
app-mon auto-group create
app-mon app-group app_group_name {add | remove} {app-name app_name | from app_name to app_name}
no app-mon app-group app_group_name
app-mon app-list {enforcement | monitor} {add | remove} {app-name app_name | app-group app_group_name}
app-mon apply
app-mon l3-mode {ipv4 | ipv6} admin-state {enable | disable}
app-mon {port chassis/slot/port[-port2]} slot chassis/slot [14-mode {tcp | udp} admin-state {enable | disable}
app-mon 14-port-exclude range-id number {tcp-service-port | udp-port} start number end number
no app-mon 14-port-exclude range-id
app-mon flow-table {enforcement | monitor} flush
app-mon flow-table enforcement stats admin-state {enable | disable}
**Application**

**Fingerprinting Commands**

- app-fingerprint admin-state {enable | disable}
- app-fingerprint {port chassis/slot/port | linkagg agg_id[-agg_id2]} {monitor-group group_name | policy-list-name policy_list | unp-profile}
- no app-fingerprint {port chassis/slot/port | linkagg agg_id[-agg_id2]}
- app-fingerprint signature-file filename
- app-fingerprint reload-signature-file
- app-fingerprint trap {enable | disable}
- show app-fingerprint configuration
- show app-fingerprint {port chassis/slot/port | linkagg agg_id}
- show app-fingerprint app-name [app_name]
- show app-fingerprint app-group [group_name]
- show app-fingerprint database {port chassis/slot/port | linkagg agg_id} [detail]
- show app-fingerprint statistics {port chassis/slot/port | linkagg agg_id}

**FCoE/FC Gateway Commands**

- fibre-channel vsan {vsan_id[-vsan_id2]} [admin-state {enable | disable}] [name description]
- no fibre-channel vsan {vsan_id[-vsan_id2]}
- fibre-channel port chassis/slot/port[-port2] mode {np | f | te} [bb-sc-n buffer_num]
- no fibre-channel port chassis/slot/port[-port2]
- fibre-channel vsan vsan_id members port chassis/slot/port[-port2]
- no fibre-channel vsan vsan_id members port chassis/slot/port[-port2]
- fcoe vsan-map vsan vsan_id [admin-state {enable | disable}] [name description]
- no fcoe vsan-map vsan vsan_id
- fibre-channel npiv-proxy load-balance static {default | dynamic-reorder | node-based}
fibre-channel npiv-proxy load-balance static {port chassis/slot/port | linkagg agg_id} fc-port
no fibre-channel npiv-proxy load-balance static {port chassis/slot/port | linkagg agg_id}
fibre-channel npiv-proxy load-balance static {port chassis/slot/port | linkagg agg_id}
no fibre-channel npiv-proxy load-balance static {port chassis/slot/port | linkagg agg_id}

VM-Snooping Commands

vm-snooping static-policing rule_name [list list_name]
no vm-snooping static-policing rule_name [list list_name]
vm-snooping logging-threshold number-of-flows [flow_num | default]
vm-snooping {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} [admin-state {enable | disable}]
no vm-snooping {port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}
show vm-snooping config
show vm-snooping port
show vm-snooping database [vxlan udp-port udp_port_num | vtep-ip ip_address] | vni vxlan_id | vm-src-mac mac_address | vm-ip ip_address [detail] [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]] [detail]
clear vm-snooping database /port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]
show vm-snooping virtual-machines
show vm-snooping filtering-resource
show vm-snooping statistics [hardware | sampling] [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]
show vm-snooping static-policy
clear vm-snooping statistics [sampling [port chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]]][hardware]

Port Mapping Commands

port-mapping_session_id [user-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} | network-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}]
no port-mapping_session_id [user-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]} | network-port {slot chassis/slot | chassis/slot/port[-port2] | linkagg agg_id[-agg_id2]}]
port-mapping_session_id [enable | disable]
no port-mapping_session_id
port-mapping_session_id [unidirectional | bidirectional]
port-mapping_session_id unknown-unicast-flooding [enable | disable]
port-mapping_session_id dynamic-proxy-arp [enable | disable]
show port-mapping [session_id] status
show port-mapping [session_id]
show ip dynamic-proxy-arp

Learned Port Security Commands

port-security {port chassis/slot/port[-port2] | chassis} | {sap {port {linkagg sap_id} [admin-state {enable | disable | locked}] | no-aging {enable | disable}} [mac-move {enable | disable}] [learn-as-static {enable | disable}] [boot-up {enable | disable}]

VXLAN Snooping Commands

vm-snooping vxlan udp-port [udp_port_num[-udp_port_num2] | linkagg agg_id[-agg_id2] | chassis]
no vm-snooping vxlan udp-port [udp_port_num[-udp_port_num2] | linkagg agg_id[-agg_id2] | chassis]
no port-security learning-window
port-security {port chassis/slot/port[-port2] | chassis} | {sap [port | linkagg] sap_id} convert-to-static
port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} mac mac_address [vlan vlan id]
no port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} mac | all | mac_address [vlan vlan id]
port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} maximum number
port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} learn-trap-threshold number
port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} max-filtering number
port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} mac-range [low mac_address | high mac_address]
no port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} mac-range [low mac_address]
port-security {port chassis/slot/port[-port2] | sap [port | linkagg] sap_id} violation
  {shutdown | restrict | discard} | violation recovery-time {default | seconds} | violation recovery-maximum {infinite | default | max_attempts}
port-security {port chassis/slot/port[-port2] | pkt-relay} no-pkt-relay
no port-security {port chassis/slot/port[-port2] | pkt-relay} no-pkt-relay
port-security pkt-relay protocol [udp] {icmp} {igmp}
port-security pkt-relay protocol udp [src-port port1[-port2]] [dst-port port1[-port2]]
show port-security pkt-relay filter
show port-security {port chassis/slot/port[-port2] | slot chassis/slot} | sap [violation | {port | linkagg} sap_id]
show port-security brief
show port-security learning-window

Port Mirroring and Monitoring Commands
port-mirroring port_mirror_sessionid source {port chassis/slot/port[-port2]} destination
  {port chassis/slot/port[-port2] | linkagg linkagg[-linkagg2]} [rpmir-vlan vlan id]
  [bidirectional | import | export | loopback] [unblocked-vlan vlan id] [tag-remove]
  [enable | disable]
port-mirroring port_mirror_sessionid no source {port chassis/slot/port[-port2] \[chassis/slot/
  port[-port2]...]
port-mirroring port_mirror_sessionid no destination {port chassis/slot/port[-port2] \[chassis/
  slot/port[-port2]...]} linkagg linkagg[-linkagg2] [linkagg[-linkagg2]...]
port-mirroring port_mirror_sessionid enable | disable
no port-mirroring port_mirror_sessionid
port-mirroring traffic-priority {normal | high}

port-monitoring port_monitor_sessionid source port chassis/slot/port[-port2] [file filename
  [size filesize] | no file | overwrite {on | off}] [import | export | bidirectional] [timeout
  seconds] [enable | disable] [capture-type {full | brief}]
port-monitoring port_monitor_sessionid no source port chassis/slot/port[-port2]
port-monitoring port_monitor_sessionid {disable | pause | resume}
no port-monitoring port_monitor_sessionid
show port-mirroring status [port_mirror_sessionid]
show port-monitoring status [port_monitor_sessionid]
show port-monitoring file port_monitor_sessionid

sFlow Commands
sflow agent ip ip_address
no sflow agent ip ip_address
vrf {name} sflow receiver receiver_index {name string | timeout {seconds | forever} | address
  {ip_address | ipv6_address | domain_name} | udp-port port | packet-size size version
  num | release}
vrf {name} sflow sampler num port chassis/slot/port[-port2] {receiver receiver_index | rate
  value | sample-hdr-size size}
no sflow sampler num port [chassis id/slot/port[-port]
vrf {name} sflow poller num port chassis/slot/port[-port] {receiver receiver_index | interval
  value}
no sflow poller num port [chassis id/slot/port[-port]
show sflow agent
vrf {name} show sflow receiver [num]
vrf {name} show sflow sampler [num]
vrf {name} show sflow poller [num]

RMON Commands
rmon probes {stats | history | alarm} [entry_number] {enable | disable}
show rmon probes {stats | history | alarm} [entry_number]
show rmon events [entry_number]

Switch Logging Commands
swlog {enable | disable | preamble | hash-time-limit seconds | duplicate-detect | console level
  num }
no swlog {preamble | duplicate-detect}
wlog syslog-server {facility | name} [vrf num]
wlog appid {all | string} [library {all | string} | subapp {all | num} | exclude {all | num}]
  {disable | enable} [level {level | num} | vrf num]
Health Monitoring Commands

ethoam association association_name domain \{domain_name | mac_address\}
  allowed-cvlan-list num\[-num2\]
no ethoam association association_name domain \{domain_name | mac_address\}
  allowed-cvlan-list num\[-num2\]
clear ethoam statistics [domain md_name association ma_name endpoint mep_id]
ethoam default-domain level num
no ethoam default-domain
ethoam default-domain mhf \{none | default | explicit\}
no ethoam default-domain
ethoam default-domain id-permission \{none | chassisid\}
no ethoam default-domain
ethoam default-domain primary-vlan \{vlan_id\} \{level \{no-level | num\}\} \{mhf \{none | default
  [explicit | defer]\} \{id-permission \{none | chassisid | defer\}\}
no ethoam default-domain
ethoam endpoint mep_id domain md_name association ma_name direction \{up | down\}
  \{port chassis/slot/port | virtual | linkagg agg_id\} \{primary-Vlan vlan_id \| cvlan cvlan_id\}
no ethoam endpoint mep_id domain md_name association ma_name
ethoam endpoint mep_id domain \{md_name | mac_address\} association ma_name admin-
  state \{enable | disable\}
ethoam endpoint mep_id domain \{md_name | mac_address\} association ma_name rfp
  \{enable | disable\}
ethoam endpoint mep_id domain \{md_name | mac_address\} association ma_name ccm
  \{enable | disable\}
ethoam endpoint mep_id domain \{md_name | mac_address\} association ma_name priority
  ccm_ltm_priority
ethoam endpoint mep_id domain \{md_name | mac_address\} association ma_name lowest-
  priority-defect lowest_priority_defect
ethoam linktrace \{target-macaddress mac_address \| target-endpoint t_mepid\}
  source-endpoint s_mepid domain \{md_name | mac_address\} association ma_name \{flag \{[fdb-
    mpid | fdbonly]\} \{hop-count hop_count\}\}
ethoam loopback \{target-endpoint t_mepid\} \{target-macaddress mac_address\}
  source-endpoint s_mepid domain md_name association ma_name \{number num\} \{data string\}
  \{vlan-priority vlan_priority\} \{drop-eligible \{true | false\}\}
ethoam fault-alarm-time centiseconds endpoint mep_id domain md_name association
  ma_name
no ethoam fault-alarm-time endpoint mep_id domain md_name association ma_name
ethoam fault-reset-time centiseconds endpoint mep_id domain md_name association
  ma_name
no ethoam fault-reset-time endpoint mep_id domain md_name association ma_name
ethoam one-way-delay \{target-endpoint t_mepid\} \{target-macaddress mac_address\}
  source-endpoint s_mepid domain md_name association ma_name \{vlan-priority vlan_priority\}
ethoam two-way-delay \{target-endpoint t_mepid\} \{target-macaddress mac_address\}
  source-endpoint s_mepid domain md_name association ma_name \{vlan-priority vlan_priority\}
clear ethoam \{one-way-delay-table | two-way-delay-table\}

Health Monitoring Commands

health threshold \{rx percent | txrx percent | memory percent | cpu percent | flash percent\}
  health interval seconds
show health configuration
show health \{port chassis/slot/port | slot chassis/slot\[-slot2\]\} \{statistics\}
show health all \{memory | cpu | rx | txrx\}

Ethernet OAM Commands

ethoam vlan vlanid_list primary-vlan vlan_id
no ethoam vlan vlanid_list
ethoam domain md_name format \{none | dnsname | mac-address-uint | string\} level num
no ethoam domain name
ethoam domain md_name mhf \{none | explicit | default\}
ethoam domain md_name id-permission \{none | chassisid\}
ethoam association ma_name format \{vpnid | unsignedint | string \| primaryvid | icc-based\}
  domain md_name
no ethoam association ma_name domain md_name
ethoam association ma_name domain md_name primary-vlan vlan_id
no ethoam association ma_name domain md_name primary-vlan vlan_id
ethoam association ma_name domain md_name mhf \{none | default | explicit | defer\}
ethoam association ma_name domain md_name id-permission \{none | chassisid | defer\}
ethoam association ma_name domain \{md_name | mac_address\} ccm-interval \{interval-
  invalid | interval100ms | interval1s | interval10s | interval1m | interval10m\}
ethoam association ma_name domain \{md_name | mac_address\} endpoint-list mep_id\[-
  mep_id2\]
no ethoam association ma_name domain \{md_name | mac_address\} endpoint-list mep_id\[-
  mep_id2\]

OmniSwitch AOS Release 8 CLI Reference Guide April 2023 page 42
show ethoam
domain md_name
show ethoam domain md_name association ma_name
show ethoam domain md_name association ma_name end-point mep_id
show ethoam default-domain configuration
show ethoam default-domain [primary-vlan vlan_id]
show ethoam remote-endpoint domain md_name association ma_name end-point s_mepid
[remote-mep r_mepid]
show ethoam cfmstack {port chassis/slot/port | virtual | linkagg agg_id}
show ethoam linktrace-reply domain ma_name
[association ma_name [end-point s_mepid]
show ethoam linktrace-tran-id domain {md_name | mac_address} association ma_name
endpoint mep_id
show ethoam vlan vlan_id
show ethoam statistics domain {md_name | mac_address} [association ma_name] [end-point mep_id]
show ethoam config-error [vlan vlan_id] [{port chassis/slot/port | linkagg agg_id}]
show ethoam one-way-delay domain md_name association ma_name end-point s_mepid
[mac-address mac_address]
show ethoam two-way-delay domain md_name association ma_name end-point s_mepid
[mac-address mac_address]

LINK OAM Commands

efm-oam admin-state {enable | disable}

show efm-oam port chassis/slot/port{-[port2]} admin-state {enable | disable}

show efm-oam port chassis/slot/port{-[port2]} mode {active | passive}

efm-oam port chassis/slot/port{-[port2]} keepalive-interval seconds

efm-oam port chassis/slot/port{-[port2]} hello-interval seconds

efm-oam port chassis/slot/port{-[port2]} remote-loopback {process | ignore}

efm-oam port chassis/slot/port{-[port2]} propagate-events {critical-event | dying-gasp}

{enable | disable}

efm-oam port chassis/slot/port{-[port2]} errored-frame-period [threshold threshold_symbols]

[window window_frames] {notify [enable | disable]}

efm-oam port chassis/slot/port{-[port2]} errored-frame [threshold threshold_symbols]

[window window_seconds] {notify [enable | disable]}

efm-oam port chassis/slot/port{-[port2]} errored-frame-seCONDS-summary [threshold

threshold_seconds] [window window_seconds] {notify [enable | disable]}

efm-oam multiple-pdu-count count

efm-oam port chassis/slot/port 11-ping [num-frames number] [delay milliseconds] [start]

show efm-oam configuration

display efm-oam port [chassis/slot/port1-port2] [enable | disable] [active | passive]

display efm-oam port chassis/slot/port detail

display efm-oam port chassis/slot/port{-[port2]} statistics

display efm-oam port statistics

display efm-oam port chassis/slot/port remote detail

display efm-oam port chassis/slot/port history [log-type { link-fault | errored-frame | errored-frame-period | errored-frame-seconds | dying-gasp | critical}]

display efm-oam port chassis/slot/port 11-ping detail

display efm-oam statistics [port chassis/slot/port{-[port2]}]

display efm-oam log-history [port chassis/slot/port{-[port2]}]

CPE Test Head Commands

test-oam string [descr description]

no test-oam string

test-oam string [direction {unidirectional | bidirectional}]

test-oam string [src-endpoint src-string] [dst-endpoint dst-string]

test-oam string port chassis/slot/port

test-oam string [vlan svlan] [{test-frame [src-mac src-address] [dst-mac dst-address]}

[direction {unidirectional | bidirectional}]}

test-oam string role {generator | analyzer | loopback}

test-oam string [duration secs] [rate rate] [packet-size bytes]

test-oam string frame

test-oam string 12-saa [priority vlan-priority] [count num-pkts] [interval inter-pkt-delay]

[continuous | size size] [drop-eligible {true | false}]

no test-oam string 12-saa

test-oam string [vlan vlan-id] [port chassis/slot/port] [packet-size bytes] start | stop]

[fetch-remote-stats]

test-oam string remote-sys-mac string

test-oam statistics flash-logging {enable | disable}

show test-oam [tests | string]

show test-oam [string] statistics

show test-oam [string] saa statistics

clear test-oam [string] statistics

test-oam group string [descr description]

no test-oam group string

test-oam group string [tests string1.......string8] [group group]

no test-oam group string

test-oam group string [src-endpoint src-string dst-endpoint dst-string | port chassis/slot/port]

[fetch-remote-stats]

test-oam group string [vlan vlan-id] [port chassis/slot/port] [packet-size bytes] start | stop]

[fetch-remote-stats]

test-oam group string [direction {unidirectional | bidirectional}]

test-oam group string [duration secs] [rate rate] [packet-size bytes]

test-oam group string [src-endpoint src-string dst-endpoint dst-string | port chassis/slot/port]

[fetch-remote-stats]
test-oam group string remote-sys-mac string
clear test-oam group string statistics
show test-oam group [tests | string]
show test-oam group [string] saa statistics
show test-oam group [string] statistics

PPPoe Intermediate Agent
pppoe-ia {enable | disable}
pppoe-ia [port {chassis/slot/port[-port2]} | linkagg agg_num] {enable | disable}
pppoe-ia [port {chassis/slot/port[-port2]} | linkagg agg_num] {trust | client}
pppoe-ia access-node-id {base-mac | system-name | mgmt-address | user-string string}
pppoe-ia circuit-id {default {atm ascii | base-mac | system-name | interface | vlan | cvlan | interface-alias | user-string string | delimiter char}
pppoe-ia remote-id {base-mac | system-name | mgmt-address | user-string string}
clear pppoe-ia statistics [port {chassis/slot/port[-port2]} | linkagg agg_num]
show pppoe-ia configuration
show pppoe-ia [port {chassis/slot/port[-port2]} | linkagg agg_num] {enabled | disabled | trusted | client]
show pppoe-ia [port {chassis/slot/port[-port2]} | linkagg agg_num] statistics

Service Assurance Agent Commands
[vrf vrf_name] saa string [desc | description] [interval interval] [jitter-threshold jitter_thresh] [rtt-threshold rtt_thresh]
[vrf vrf_name] no saa string
[vrf vrf_name] saa string type ip-ping destination-ip ip_address source-ip ip_address type-of-service tos [num-pkts count] [inter-pkt-delay delay] [payload-size size]
saa string type mac-ping destination-mac mac_address vlan vlan_id [vlan-priority vlan_priority] [drop-eligible [true | false]] [data data [num-pkts count] [inter-pkt-delay delay] [payload-size size] [isid-check isid]
saa spb [auto-create] [auto-start] [interval interval] [vlan-priority vlan_priority] [drop-eligible [true | false]] [data data [num-pkts count] [inter-pkt-delay delay] [payload-size size] [jitter-threshold jitter_thresh] [rtt-threshold rtt_thresh] [keep]
saa spb reset
saa spb flush
saa string type ethoam-loopback {target-endpoint t_mepid | target-mac-address mac_address} source-endpoint s_mepid domain md_name association ma_name vlan-priority vlan_priority [drop-eligible [true | false]] [data data [num-pkts num] [inter-pkt-delay delay]
saa string type {ethoam-two-way-delay} {target-endpoint t_mepid | target-mac-address mac_address} source-endpoint s_mepid domain md_name association ma_name vlan-priority vlan_priority [num-pkts num] [inter-pkt-delay delay]
[vrf vrf_name] saa string start [at yyyy-mm-dd hh:mm:ss]

CMM Commands
reload [chassis-id chassis] secondary [in [hours:] minutes] [at hour:minute [month day | day month]]
reload secondary cancel
reload [chassis-id chassis] all [in [hours:] minutes] [at hour:minute [month day | day month]]
reload all cancel
reload [chassis-id chassis] from image_dir [rollback-timeout minutes] [no rollback-timeout]
reload slot chassis/slot
reload chassis-id chassis [all] [in [hours:] minutes] [at hour:minute [month day | day month]]
reload chassis-id cancel
copy certified image_dir [make-running-directory]
issu from image_dir [redundancy-time minutes]
issu slot num
write memory [flash-synchro]
copy running certified [flash-synchro]
modify running-directory image_dir
copy flash-synchro
takeover [chassis]
show running-directory
show reload [chassis-id chassis] [status | all status]
show microcode [working | certified | loaded | issu | image_dir]
usb [enable | disable]
usb backup admin-state [enable | disable] [{key string | hash-key string [bootable]}
usb auto-copy [enable | disable] copy-config [enable | disable] [key string | hash-key string]
mount [/uflash]
unmount /uflash
show usb statistics
show issu status
auto-config-abort
image integrity check image_dir key-file filename
Chassis Management and Monitoring Commands

system contact text_string
system name text_string
system location text_string
system date [mm/dd/yyyy]
system time [hh:mm:ss]

update boot {cmm slot} | {all | slot} file filename
update fpga-cpld {cmm} | {chassis/cmm | all} | {chassis/ni | daughter num} file filename
reload slot slot
power slot chassis/slot
no power slot chassis/slot
powersupply enable [slot]
powersupply powersave {enable | disable}
powersupply num name string type {ALE {xl-ac | lo-ac | hi-ac} | phoenix-contact {48VDC | 24VDC}} | third-party wattage num {chassis-id chassis_id}
hash-control {brief | extended [udp-tcp-port] | load-balance non-ucast {enable | disable}}
hash-control extended no udp-tcp-port
bluetooth {admin-state {enable | disable} | transmit-power {low | high}}
capability profile {switch | router}
capability profile tcam mode {source-ipv6 | dest-ipv6}
capability trap-threshold {MAC | ARP} {HIGH num | LOW num}
capability shared-vlan-learning {enable | disable}
uboot access {enable | disable}
uboot authentication {enable password password | disable}
license apply {file file_name | key license_key} [order-id order_id]
show system
show hardware info
show chassis
show cmm [slot]
show slot [slot]
show module [slot]
show module long [slot]
show module status [slot]
show powersupply [slot]
show fan [slot]
show fantray [slot]
show hash-control [non-ucast]
appmgr {start | stop | restart} [ams broker | config-sync | config-dbase | ams cron-app] [ams-apps iot-profiler] [aos-ovsdb ovsdb-app]
appmgr list [app_name]
show appmgr
appmgr commit
pkgmgr {install | verify} package_file_name | remove package_name
show pkgmgr [package_name]
pkgmgr commit

Network Time Protocol Commands

ntp server {ip_address | server_name} [key key_id | | minpoll poll | maxpoll poll | version
version | prefer | burst | iburst | preempt]
no ntp server ip_address
ntp server synchronized
ntp server unsynchronized
ntp client admin-state {enable | disable}
ntp src-ip preferred {default | no-loopback0 | ip_address}
no ntp src-ip preferred
ntp broadcast-client {enable | disable}
ntp broadcast-delay microseconds
ntp key key {trusted | untrusted}
ntp key load
ntp authenticate {enable | disable}
ntp master stratum_number
ntp interface {interface_ip} {enable | disable}
ntp max-associations number
ntp broadcast {broadcast_addr} [version version] [minpoll poll_interval]
no ntp broadcast {broadcast_addr}
ntp peer {ip_address} [key key_id] [version version] [minpoll poll_interval]
no ntp peer {ip_address}
ntp vrf-name name
show ntp status
show ntp client
show ntp client server-list
show ntp server client-list
show ntp server status {ip_address}
show ntp keys
show ntp peers
show ntp server disabled-interfaces

Session Management Commands

session login-attempt integer

File Management
Commands

cd [path]
pwd
mkdir [options] [path] /dirname
rmdir [options] dirname
ls [options] [path/filepath]
rm [options] [path/filepath]
Web Management Commands

- cp [options] source destination
- scp [options] user_name@remote_ip_addr:[path]source [path]target
- mv [options] source destination
- chmod [+w | -w] [path]/file
- fsck /uflash {repair | no-repair}
- newfs /uflash
- vi [options] [path]/filename
- tty lines columns
- show tty
- tftp [options] host [port]
- sftp [options] [ip_address]
- ftp [port [default | service_port] | admin-state [enable | disable] | ip_address]
- show ftp

SNMP Commands

- snmp station {ip_address | ipv6_address | domain_name} {[port] | [username] [v1 | v2 | v3 | v3 tsm] local-identity local_string remote-identity remote_string} [enable | disable]
- no snmp station {ip_address | ipv6_address | domain_name}
- show snmp station [details]
- show snmp-engineid-type {text | mac-address} ipv4-address | ipv6-address
- snmp-engineid {text_string | mac_address | ipv4_address | ipv6_address}
- show snmp-engineid
- snmp community-map {[flash-key string | community_string] user useraccount_name} [enable | disable]
- no snmp community-map community_string
- show snmp community-map
- show snmp security {tsm | no-security | authentication set | authentication all | privacy set | privacy all | trap-only | tls [enable | disable]}
- snmp security tsm [enable | disable]
- snmp tsm-map remote-identity remote_string user_string
- show snmp tsm-map
- show snmp security [tsm]
- show snmp statistics
- show snmp mib-family [table_name]
- show snmp trap absorption [enable | disable]
- show snmp-trap to-webview [enable | disable]
- show snmp-trap replay-ip {ip_address | ipv6_address | domain_name} [seq_id]
- show snmp-trap filter-ip {ip_address | ipv6_address | domain_name} trap_id_list
- show snmp-trap filter-ip {ip_address | ipv6_address | domain_name} trap_id_list
- show snmp authentication-trap [enable | disable]
- show snmp-trap replay-ip
- show snmp-trap filter-ip
- show snmp authentication-trap
- show snmp-trap config
- show event-action [statistics | trap name [statistics]]
- show event-action [statistics]
- show event-action [statistics | trap name [statistics]]

OmniVista Cirrus Commands

- cloud-agent admin-state {enable | disable | force | restart}
- cloud-agent discovery-interval minutes
- cloud-agent remove-inconsistent-certificate
- show cloud-agent status
- show cloud-agent vpn status
naas license call-home interval {minutes | now}
naas license apply file_name
show naas license
show naas-agent status

OpenFlow Commands

openflow back-off-max seconds
openflow idle-probe-timeout seconds
openflow logical-switch name [probe-time num | failure-detect-time num | tcp-buffer-size num | dpid string] [admin-state {enable | disable}] [mode {normal | api | pfc-channel}] [version {1.0 | 1.3.1}+] [learned-mac-update {enable | disable}] [vlan vlan_id] [table-miss-action {drop | controller}]
no openflow logical-switch <name>
openflow logical-switch name controller {ip_address | domain_name} [:port] [priority num] admin-state {enable | disable}
no openflow logical-switch name controller {ip_address | domain_name} [:port]
openflow logical-switch name interfaces {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2] | [type {trunk | access}] | [native-vlan vlan] | [vlan-tag vlan][-vlan2]}]
no openflow logical-switch name interfaces {port chassis/slot/port1[-port2] | linkagg agg_id[-agg_id2]}
show openflow
show openflow logical-switch [name | controllers | interfaces [vlans | port | linkagg] | details]

DNS Commands

ip domain-lookup
no ip domain-lookup
ip name-server server_address1 [server_address2 [server_address3]]
ipv6 name-server server_ipv6_address1 [server_ipv6_address2 [server_ipv6_address3]]
ip domain-name name
no ip domain-name
show dns
Index

Numerics
802.1ab 17-1
  notification of local system MIB changes 17-14
  reinit delay 17-8
  show port statistics 17-46
  tlv management 17-21, 17-38, 17-40, 17-42
  transmit time interval 17-4
802.1p
  mapped to ToS or DSCP 37-177
  QoS port default 36-51

A
AAA 39-1
  password-size min 39-69
  show user network profile 40-188, 40-196, 40-204,
    40-254, 40-357, 40-367, 40-370, 40-375,
    40-378, 40-380, 40-382, 40-389, 40-393, 40-396,
    40-415, 40-417, 40-419, 40-421, 40-423
Access-Node-Identifier 1-8
  accounting 1-70
  actions
    supported by hardware 37-154
    active login sessions 6-33
  Alcatel Mapping Adjacency Protocol 18-1
  alerts 51-6
  AMAP
    see Alcatel Mapping Adjacency Protocol
ASA Configuration
  verify information about 39-45
  assigning ports to VLANs 5-4

B
BGP 30-1
  aggregate routes 30-40
  autonomous system 30-10, 30-39
  communities 30-46, 30-58
  confederation 30-30
  fast external failover 30-18
  load 30-6
  local preference 30-16
  MED 30-62, 30-269
  neighbor 30-64, 30-66, 30-275, 30-277, 30-285, 30-349
  policy 30-136
  route dampening 30-35
  route reflectors 30-24
boot.cfg file
  QoS log lines 36-10
BPDU
  see Bridge Protocol Data Units
Bridge Protocol Data Units 8-3, 8-57, 8-59, 8-61, 8-63

C
CCM
  priority value 53-40
  transmission interval 53-19
  transmission rate 53-38
  circuit-id
    ascii 1-10
    cvlan 1-10
    delimeter 1-10
CLI
  logging commands 6-26, 6-51–6-53
  client 1-6
  CMS
    running configuration 3-11
    takeover 3-22
  CMS 4-92
    allocated addresses 4-94
    mac-range 4-92
    range table 4-92
  commands
    domains and families 39-140
    conditions
      multiple conditions defined 37-46, 37-136
    Continuity Check Messages
      see CCM
    current user session 6-31

D
Data Center Bridging 36-2
DCB
  see Data Center Bridging
drug messages 51-6
DHCP Relay 25-1
  DHCP server IP address 25-39
  elapsed boot time 25-14
  forward delay time 25-14
  Global DHCP 25-39
  maximum number of hops 25-16, 25-88
  per-VLAN forwarding option 25-44
  show ip helper 25-26, 25-46
  standard forwarding option 25-43
directory
  change 7-2
  create 7-6
  delete 7-8
  display 7-4, 7-10, 7-21, 7-24
DNS
  domain name 66-2
  enables resolver 66-2
  name servers 66-3, 66-4, 66-9, 66-11
  resolver 64-1, 66-1
DSCP
  mapped to 802.1p or ToS 37-177
  QoS port default 36-53
DVMRP
interface 33-7
neighbor 33-13
status 33-3
dynamic link aggregation
   adding ports 12-39
   creating 12-18
   deleting 12-18
   deleting ports 12-39
   LACPDU frames 12-42, 12-49
   local port MAC address 12-45
   remote group MAC address 12-33
   remote port MAC address 12-52

E
editor
   vi 7-27
error file 9-4
error frame 1-75
errors 51-6
Ethernet 1-1
   flow 1-4, 1-45, 1-47, 1-49, 1-139, 1-144, 1-146
   interfaces 1-6
   trap port 1-4, 1-45, 1-47, 1-49, 1-139, 1-144, 1-146
   ethernet domain 53-5, 53-60, 53-62
Ethernet OAM 53-1
   association endpoint list 53-21, 53-23
   lowest priority fault alarm 53-32, 53-42, 53-44
   maintenance association 53-11, 53-13
exit 6-30

F
Fadvrout.img file 34-5, 34-9
fault alarm
   alarm time 53-50
   reset time 53-52
Fibre Channel
   FCoE Initiation Protocol 43-1
   FCoE/FC Gateway 44-1
   FIP Snooping 43-1
file
   copy 7-14, 7-16
   delete 7-12, 7-25
   move 7-18
   privileges 7-20
   system check 7-22, 7-23
   transfer 7-32, 7-36

H
health 52-2
high availability VLANs
   egress ports 6-2, 6-4, 6-5, 6-6, 6-7, 6-8, 6-10
i
IGMP
   default 32-8
   group entry 32-19, 32-169, 32-178
ip multicast querier-forwarding 32-43
last member query interval 32-23
neighbor entry 32-15, 32-172
querier entry 32-17, 32-175
query interval 32-21
query response interval 32-25, 32-27
querying 32-33, 32-43
robustness variable 32-35
router timeout 32-29
source timeout 32-31
spoofing 32-37, 32-39
zapping 32-41, 32-45
interior gateway protocol
   OSPF 27-1, 28-1, 29-1
Intermediate Agent 1-1
IP
   interface tunnel 20-11
IP Multicast Switching
   see IPMS 32-1
IPMS 32-1
   ipv6 multicast querier-forwarding 32-121
ipv6
   address 21-13
dad-check 21-19
hop-limit 21-20
interface 21-3
interface tunnel source destination 21-15
neighbor 21-23, 21-24
ping6 21-44
pmtu-lifetime 21-20, 21-22
prefix 21-26, 21-34
rip 23-43
route 21-36
traceroute 21-51
ISIS 29-1
   authentication check 29-10

L
LACP
   see dynamic link aggregation
Link Trace Messages 53-46
   priority value 53-40
link-state protocol
   OSPF 27-1, 28-1, 29-1
LPS 47-1
   learning-window 47-5
   learn-trap-threshold 47-16
   max-filtering 47-18
   maximum 47-14

M
MAC address table
   duplicate MAC addresses 4-19, 4-21, 4-23, 4-25, 4-27
MAC address VLAN rule 40-196, 40-201, 40-204
MAC addresses
   aging time 4-31
   dynamic link aggregation 12-33, 12-45, 12-52
   statically assigned 4-18, 4-20, 4-29
Maintenance Association
  create 53-11, 53-13
  modify 53-21

Maintenance Intermediate Point
  see MIP

Management Domain
  display all information 53-4, 53-6, 53-7, 53-10, 53-59, 53-62, 2-3, 2-5, 2-8, 2-11, 2-13, 2-14, 2-17, 2-20, 2-22, 2-24, 2-26, 2-28, 2-30, 2-42, 2-45
display specific information 53-6, 53-10, 53-61, 2-3, 2-5, 2-8, 2-17, 2-20, 2-22, 2-24

MEP
  administrative state 53-21, 53-34
  MHF value 53-7

MLD
default 32-85
group entry 32-97, 32-206, 32-215
last member query interval 32-101
neighbor entry 32-93, 32-209
querier entry 32-95, 32-212
query interval 32-99
query response interval 32-103, 32-105
querying 32-111
robustness variable 32-113
router timeout 32-107
source timeout 32-109
spoofing 32-115, 32-117
zapping 32-119, 32-123

mobile ports
  trusted ports 36-5

modules
  power 4-23
  reloading 3-4
  temperature 4-28

multicast routing
  show routing information 35-17
  multicast address boundaries 35-13

multicast routing
  boundary 35-3
datagram ttl threshold 35-11
interface ttl 35-7, 35-11
ipv6 next-hop information 35-25

MVRP 16-1
  applicant 16-10
disable globally 16-2
display configuration on specified link aggregate 16-33
display configuration on specified port 16-30
dynamic VLANs 16-7
enable globally 16-2
enable on specified link aggregate 16-5
enable on specified port 16-3
registration 16-8

N
  Network Interface (NI) modules
    reloading 4-18, 4-20, 4-22

NTP 5-1
  broadcast delay 5-15, 5-29

O
  OSPF
    area 27-25
global 27-4
  graceful restart 27-63, 28-73
  interface 27-31
  link-state protocol 27-1, 28-1, 29-1

P
  pending configuration
    commands associated with 36-33
    erasing policy configuration 36-33
  pim
cbcr 34-17
ipv6 pim sgroute 34-214
ipv6 pim sparse mode 34-180
max-rps 34-29, 34-90, 34-182
neighbor loss notification period 34-57
probe-time 34-31, 34-90
register-suppress-timeout 34-41, 34-90, 34-182
rp-candidate 34-25
rp-threshold 34-25
show pim notifications 34-119
sparse status 34-5, 34-7, 34-90, 34-93, 34-183
split status 34-45, 34-90, 34-161, 34-182
ssm group 34-13
static-rp 34-19, 34-21
PIM-SM v2 34-33

PMM
  port mirroring 48-2
  port monitoring source 48-9

Policies
  save option 37-5
  policy condition
dscp 37-98
  source vlan 37-108

Policy servers
  displaying information about 38-6
  SSL 38-4

port mapping 46-2
PPPoE Intermediate Agent 1-1

Q
  QOS
    ip phone traffic 36-15
    quarantine path 40-277
**R**

remote-id 1-13, 1-18
resolver
   see DNS resolver
RIP
   active peer 23-41
   forced hold-down timer 23-21
   garbage timer 23-31
   global 23-3
   hold-down timer 23-32
   host-route 23-23
   IGP 23-1
   interface 23-7
   invalid timer 23-30
   route-tag 23-24
   security 23-25
   status 23-5
RMON
   probes 50-2

**S**

secure shell session 6-42, 6-43, 7-35
secure socket layer
   see SSL
Server Load Balancing 31-1
   adding clusters 31-5
   adding servers 31-17
   deleting clusters 31-5, 31-17
   disabling 31-2
   enabling 31-2
   server administrative status 31-17
Service Manager 10-1
   session management
      banner 6-7
      kills 6-28
      login attempt 6-3
      more 6-39
      prompt 6-13, 6-14
      timeout 6-9
      user profile 6-20
      xon-xoff 6-16, 6-17
sFlow 49-7
   poller 49-9
   receiver 49-3
   sampler 49-7
Shortest Path Bridging 9-1
   backbone VLAN 9-3
   services 10-1
SLB
   see Server Load Balancing
smurf attack 20-32
snapshot 9-11
SNMP
   community map 10-12, 10-49
   community strings 10-12
   security 10-18
   station 10-3
   statistics 10-27
   trap 10-31
source learning 4-1
   MAC address table 4-1, 4-18, 4-20, 4-29
Spanning Tree Algorithm and Protocol 8-1
   1x1 operating mode 8-3, 8-9, 8-11, 8-15, 8-17, 8-112
   bridge ID 8-20
   flat operating mode 8-3, 8-9, 8-11, 8-15, 8-17, 8-112
   port states 8-46, 8-50
   pvst+ mode 8-32
Spanning Tree port parameters
   connection type 8-52, 8-53, 8-54, 8-55, 8-57, 8-59, 8-60,
   8-63, 8-64, 8-65, 8-66, 8-67, 8-68, 8-69, 8-70, 8-71
   link aggregate ports 8-36, 8-39
   mode 8-46, 8-50
   path cost 8-46, 8-50
   Spanning Tree status 8-36, 8-38
SPB
   see Shortest Path Bridging
ssh6 6-45, 6-46, 6-47, 6-49, 6-50
SSL 8-6
   policy servers 38-4
   static link aggregation
      creating 12-3
      deleting 12-3
   static MAC addresses 4-18, 4-20, 4-29
   syntax check 9-9
   system information
      administrative contact 4-4
      date 4-10
      location 4-8
      name 4-6
      time 4-10, 4-12
      time zone 4-14
T
telnet 6-40
timer session 9-6
Time-To-Live
   see TTL
ToS
   mapped to 802.1p or DSCP 37-177
   QoS port default 36-53
   trust 1-6
   TTL 35-7, 35-11

U
UDLD 3-1
   clear UDLD statistics 3-12
   probe-message advertisement timer 3-8
   show global status 3-13
   show neighbor ports 3-20
   user accounts
      SNMP access 39-62
      UTC 5-1

V
VLAN rules
MAC address  40-196, 40-201, 40-204

VLAN Stacking
  display list of all or range of configured SVLANs  7-43, 7-48, 7-49, 7-78
  ethernet-service sap  7-12
  ethernet-service uni-profile  7-23, 7-27, 7-35, 7-37, 7-39

VLANs  5-1, 5-2, 14-1
  administrative status  5-2, 5-16
  default VLAN  5-4
  description  5-2, 9-3
  FCoE  43-15
  port assignments  5-4
  secondary VLAN  5-4
  Spanning Tree status  8-7

VRRP
  accept  26-26
  configure address  26-7
  configure/modify  26-3
  delay  26-16
  display configuration  26-42
  display statistics  26-46
  display track-association  26-52
  display tracking policies  26-50
  group  26-33
  preempt  26-24
  priority  26-22
  set  26-30
  show vrrp group-association  26-57
  track-association  26-14
  tracking policy  26-9
  version  26-18

VXLAN
  VM Snooping  45-1
  VXLAN Snooping  45-1

W
  warnings  51-6

WebView
  enabling/disabling  8-2, 8-4